Information Systems Security Handbook

Contents

Part-I Information Technology Security Policy of IAAD

Information Technology Security Policy

1. Preamble

The Indian Audit and Accounts Department acknowledges an obligation to ensure appropriate security for all Information Technology data, equipment, and processes in its domain of ownership and control. The purpose of this Security Policy is to create an environment that ensures security of equipments, maintain system security and availability, data integrity, and individual privacy by preventing unauthorized access to information and information systems and by preventing misuse of, damage to, or loss of data.

This Policy will:

1. Enumerate the elements that constitute IT security.

2. Explain the need for IT security.

3. Specify the various categories of IT data, equipment, and processes subject to this policy.

4. Indicate, in broad terms, the IT security responsibilities of the various roles in which each member of the Department may function.

5. Indicate appropriate levels of security through instructions in the form of policies and guidelines.

2. Reasons for IT Security

The objective of information security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity".

Availability means the characteristic of data, information and information systems being accessible and useable on a timely basis in the required manner.

Confidentiality means the characteristic of data and information being disclosed only to authorized persons, entities, and processes at authorized times and in an authorized manner.

Integrity means the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness by protecting the data and information from unauthorized, unanticipated, or unintentional modification.

Confidentiality of information may be mandated by common law, formal statute, explicit agreement, or convention. Different classes of information warrant different degrees of confidentiality.

The hardware and software components that constitute the Department's IT Assets represent a sizable monetary investment that must be protected. The same is true for the information stored in its IT systems, some of which have taken huge resources to generate, and some of which can never be reproduced.

The assets that must be protected include:

- Computer and Peripheral Equipment.
- Communications Equipment.
- Computing and Communications Premises.
- Supplies and Data Storage Media.
- System Computer Programs and Documentation.
- Application Computer Programs and Documentation.
- Information.

The use of IT assets in a manner other than for the purpose for which they were intended represents a misallocation of valuable resources, and possibly a danger to the Department's reputation or a violation of the law.

Efficient and Appropriate Use ensures that the Departmental IT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others.

Finally, proper functioning of IT systems is required for the efficient operation of the Department. Some systems, such as the Voucher Level Computerization Application, and the General Provident Fund Application are of paramount importance to the functioning of the Department.

3. Security Philosophy

While the basic security principles are to protect the confidentiality, integrity, and availability of the information and information resources within the Indian Audit and Accounts Department, the security endeavour would be governed by the following Core Principles:

1. Awareness: Employees should be aware of the need for security of information systems and networks and what they can do to enhance security. Employees should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency.

2. Responsibility: All Employees are responsible for the security of information systems and networks. They should be accountable in a manner appropriate to their individual roles. Organisations should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

3. Response: Employees should act in a timely and co operative manner to prevent, detect and respond to security incidents. Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, Employees should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents.

4. Ethics: Employees should respect the legitimate interests of others. Given the pervasiveness of information systems and networks, Employees need to recognise that their action or inaction may harm others, and therefore, strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others.

5. Democracy: The security of information systems and networks should be compatible with essential values of a democratic society. Security should be implemented in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

6. Risk assessment: Risk assessments should be conducted at regular intervals. Risk assessment identifies threats and vulnerabilities and should be sufficiently broad based to encompass key internal and external factors, such as technology, physical and human factors, policies and third party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

7. Security design and implementation: Employees should incorporate security as an essential element of information systems and networks. Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm to data and equipments from identified threats and vulnerabilities. Both technical and non technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation’s systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

8. Security management: Organisation should adopt a comprehensive approach to security management. Security management should be based on risk assessment and should be dynamic, encompassing all levels of Organisation’s activities and all aspects of their operations. It should include forward looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security.

9. Reassessment: Organisation should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. New and changing threats and vulnerabilities are continuously discovered. Organisation should continually review, reassess and modify all aspects of security to deal with these evolving risks.

4. Policy Statement:

It is the Policy of the organization to ensure that:

1. Assets will be classified as to the level of protection required;

2. Information will be protected against unauthorized access;

3. Confidentiality of information will be assured;

4. Integrity of information will be maintained;

5. Business requirements for the availability of information and information systems will be met.

6. Personnel security requirements will be met;

7. Physical, logical, and environmental security (including communications security) will be maintained;

8. Legal, regulatory, and contractual requirements will be met;

9. Systems development and maintenance will be performed using a life cycle methodology;

10. Business continuity plans will be produced, maintained, and tested;

11. Information security awareness training will be provided to all staff;

12. All breaches of information systems security, actual or suspected, will be reported to, and promptly investigated by Information Security Officer; and

13. Violations of Information Security Policy will result in penalties or sanctions.

To ensure that the above objectives are adequately covered, and protection to the Information Assets are commensurate to the likely harm from security failures, Risk Assessment would be conducted periodically for all IT Assets of the Department. This would be reviewed at intervals no later than once in three years.

5. Roles and Responsibilities:

1. Policy Management: This policy has been approved by the Comptroller and Auditor General of India. Formulation and maintenance of the policy is the responsibility of the Director/Dy. Director, (Information Systems) of the office of the CAG of India, who will also function as the Information Security Officer of the Department.

2. Policy Implementation.

- Each member of the Department will be responsible for meeting published IT Security standards.
- The Safety and Security of each IT Asset would be the primary responsibility of the Head of the Office.
- Each office would have one Group officer designated as the IT Security manager for ensuring compliance with the various Guidelines and policies enunciated by this document.

3. Individuals.

- All ordinary users of the IT resources are responsible for the proper care and use of IT resources under their direct control, and must comply with the provisions of the IT Policy
- Individuals will be custodians of desktop systems under their control

6. Policy Documentation.

This policy is enunciated by the Security Handbook organized in four parts:

1. Part-I: IT Security Policy

2. Part-II: Domain Specific Security Instructions.

3. Part-III: Subsidiary Security Policies. This has to be read along with the Domain specific instructions given in Part-II.4. Part-IV: Guidelines and Methodologies.

Additional procedures and Guidelines would be issued from time to time to supplement the security handbook.

7. Changes

The IT Security Policy is a "living" document that will be altered as required to deal with changes in technology, applications, procedures, legal and social imperatives, perceived dangers, etc. The policy would be reviewed annually, and required changes made with the approval of the Comptroller and Auditor General of India.

Part-II

Domain Specific Security Instructions

1. Organizational Security 1.1 Guiding PrinciplesInformation Security Infrastructure Objective: To manage information Security within the organization. A management framework should be established to initiate and control the implementation of information security within the organization. Suitable management fora with management leadership should be established to approve the information security policy, assign security roles and co-ordinate the implementation of security across the organization. If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when dealing with security incidents. A multi-disciplinary approach to information security should be encouraged, e.g. involving the co-operation and collaboration of managers, users, administrators, application designers, auditors and security staff, and specialist skills in areas such as insurance and risk management. Security of Third Party Access Objective: To maintain the security of organizational information processing facilities and information assets accessed by third parties. Access to the organisation's information processing facilities by third parties should be controlled. Where there is a business need for such third party access, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in a contract with the third party. Third party access may also involve other participants. Contracts conferring third party access should include allowance for designation of other eligible participants and conditions for their access. Outsourcing Objective: To maintain the security of information when the responsibility for information processing has been outsourced. Outsourcing management should address the risks, security controls and procedures for information systems, networks and/or desktop environments in the contract between parties. General: An information security infrastructure protects an institution's information assets by defining assets and the necessary

resources to protect them, and assigning responsibility for assets. This infrastructure must consist of information security organizations and programs that ensure the confidentiality, availability, accountability, and integrity of information assets. Director/Dy. Director (IS) would be the Information Security Officer of the Indian Audit and Accounts Department. Important Security related issues would be addressed by a Management Information Security forum comprising of the Principal Director(IT Audit), Director(IS), and IT Advisor. While the Information Security Officer would be responsible for framing the policies and guidelines, the primary responsibility for protection of IT Assets in each office would be with the Head of the Office (Accountant General/ Principal Director). The head of the office shall designate one of the Group officers as the IT Security Manager of the office responsible for addressing the security concerns relevant to the IT Assets. This may be the Group Officer in charge of the single largest IT Application running in the office. For example, in case of Accounts office, this would be the DAG/Sr.DAG holding the charge of Accounts and VLC.The IT Security Manager at each office would ensure compliance with the security procedures for the IT Asset.

1.2 Security InstructionsFormation of IT Support Cell: Each office shall maintain an EDP Cell which would provide specialist IT Support to various IT Applications running in the office. The EDP Cell would not be directly be linked to any functional wing, but report to the Group Officer designated as IT Security Manager of the office. Specifying information security requirement for new Hardware: All purchases of new systems hardware or new components for existing systems must be made in accordance with Information Security Policy and associated guidelines. Such requests to purchase must be based upon a User Requirements Specification document and take account of longer term organizational business needs. The system must have adequate capacity or else it may not be able to process the data. Specifying detailed functional need for new hardware: Except for minor purchases, hardware must be purchased through a structured evaluation process. Information Security features and requirements must be identified. Testing Systems and Equipment: All equipment must be fully and comprehensively tested and formally accepted by EDP Cell of the office before being transferred to the live environment. Appointing System Administrators: The organisation's systems are to be managed by a suitably qualified systems administrator who is responsible for overseeing the day to day running and security of the systems. Each office should appoint such a qualified system administrator from among the office staff, not below the post of Section Officer, or Data Processor. Administrating Systems: System Administrators must be fully trained and have adequate experience in the wide range of systems and platforms used by the organisation. In addition, they must be knowledgeable and conversant with the range of Information Security risks which need to be managed. The System Administrator must receive an adequate level of training on the system within their area of responsibility. The System Administrator must also be familiar with the Information Security risks associated with the system administration function. Specifying User Requirements for Software: All requests for new applications systems or software enhancements must be presented to senior management with a Business Case with the business requirements presented in a User Requirements Specification document. Establishing Ownership for System Enhancements: All proposed system enhancements must be business driven and supported by an agreed Business Case. Ownership (and responsibility) for any such enhancements will intimately rest with the business owner of the system. Justifying New System Development: The development of new/from the scratch software is only to be considered, if warranted by a strong Business Case and supported both by management and adequate resources over the projected life time of the resultant project. Acquiring Vendor Developed Software: Vendor developed software must meet the User Requirements Specification and offer appropriate product support. Permitting Third Party Access: Third party access to organisational information is only permitted where the information in question has been sufficiently protected and the risk of possible unauthorised access is considered to be negligible. Commissioning Facilities Management : Any Facilities Management company must be able to demonstrate compliance with this organisation’s Information Security Policies and also provide a Service Level Agreement which documents the performance expected and the remedies available in case of non compliance. Contracting with External Suppliers / other Service Providers: All external suppliers who are contracted to supply services to the organization must agree to follow the Information Security policies of the organization. An appropriate summary of the Information Security Policies must be formally delivered to any such supplier, prior to any supply of services. The implementation of Information Security within each office of IAAD would be reviewed annually by ITA, and the report forwarded to the Information Security Officer after discussion on the same with the Head of the office. The Information Security Officer would conduct Security Audits of selected offices such as to cover each large IT Application at least once every year.

2. Asset Classification and Control

2.1 Guiding PrinciplesAccountability for assets Objective: To maintain appropriate protection of organizational assets. All major informational assets should be accounted for and have a nominated owner. Accountability for assets helps to ensure that appropriate protection is maintained. Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned. Responsibility for implementing controls may be delegated. Accountability should remain with the nominated owner of the asset.

Information ClassificationObjective: To ensure that information assets receive an appropriate level of protection. Information should be classified to indicate the need, priorities and degree of protection. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification system should be used to define an appropriate set of protection levels, and communicate the need for special handling measures.

GeneralEach office shall maintain an inventory of IT Assets. The IT Assets would include applications, computer equipments, communication equipment etc. The overall responsibility for the IT Asset in each office would rest on the head of the office (Accountant General/ Principal Director). The ownership of the IT Asset would lie with the Group officer in charge of the function. The Security issues relevant to the IT Asset would however be the responsibility of the designated IT Security Manager.

Information within IAAD would bear one of the following classifications:Unclassified - data that does not fall into any of the other data classifications noted below. This data may be made generally available without specific data custodian approval. Operational Use Only - data whose loss, corruption or unauthorized disclosure would not necessarily result in any financial or legal loss BUT which is made available to data custodian approved users only. Private - data whose disclosure would not result in any financial or legal loss to the organisation BUT involves issues of personal credibility, reputation, or other issues of personal privacy. Restricted - data whose loss, corruption or unauthorized disclosure would tend to impair the function of the Organisation, or result in financial, or legal loss. Confidential - data whose loss, corruption or unauthorized disclosure would be a violation of Union / State laws /regulations. The responsibility for defining the classification of an item of information would be with the originator or nominated owner of the information. Access control decisions would be based on the Information Classification detailed above.

2.2 Security Instructions Managing and Using Hardware Documentation: Hardware documentation must be kept up-to-date and readily available to the staff who are authorised to support or maintain systems (EDP Cell of the Office). Documentation refers to both the operator manuals and the technical documentation that should be provided by the supplier / vendor.Maintaining a Hardware Inventory or Register: A formal Hardware Inventory of all equipment is to be maintained and kept up to date at all times. This data has to be maintained electronically in a database application. All computer hardware should prominently bear suitable bar-coded identification. The hardware register (electronic/manual) has to be audited annually by an IAAS officer belonging to some other office. Defining Information: Each office of the Indian Audit and Accounts Department must record, maintain and update a data base of its information assets, along with the designated owner of the asset. Transporting Sensitive Documents: The designated owners of documents which contain sensitive information are responsible for ensuring that the measures taken to protect their confidentiality, integrity and availability, during and after transportation / transmission, are adequate and appropriate. Labelling Classified Information: All information, data and documents of classification level Restricted or Confidential are to be clearly labelled so that all users are aware of the ownership and classification of the information. Storing and Handling Classified information: All information, data and documents must be processed and stored strictly in accordance with the classification levels assigned to that information. Isolating Top Secret Information: All information, data or documents classified as highly sensitive (Restricted/Confidential) must be stored in a separate secure area.

3. Personnel Security 3.1 Guiding Principles Security in job definition and resourcing Objective: To reduce the risks of human error, theft, fraud or misuse of facilities. Security responsibilities should be addressed at the recruitment stage, included in contracts, and monitored during and individual’s employment. Potential recruits should be adequately screened, especially for sensitive jobs. All employees and third party users of information processing facilities should sign a confidentiality (non-disclosure) agreement. User Training Objective: To ensure that users are aware of Information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work. Users should be trained in security procedures and the correct use of information processing facilities to minimize possible security risks. Responding to Security incidents and malfunctions Objective: To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents. Incidents affecting security should be reported through appropriate management channels as quickly as possible. All employees and contractors should be made aware of the procedures for reporting the different types of incident (security breach, threat, weakness, or malfunction) that might have an impact on the security of organizational assets. They should be required to report any observed or suspected incidents as quickly as possible to the designated point of contact. The organization should establish a formal disciplinary

process for dealing with employees who commit security breach. To be able to address security breach properly, it might be necessary to collect evidence as soon as possible after the occurrence. General Users of IT resources should be aware of potential security concerns and understand their responsibility to report security incidents or vulnerabilities. All users of IT System in IAAD should report security incidents involving breach in security, security weakness, or software malfunctions to the Group officer in charge of the IT Security. The User providing such information on breach of security would be assured of confidentiality. The report should include the following: · Incident type· Severity level· Access details· InvolvementThe Security breach, if found serious should be noted, and the rectification response should be recorded in a historical database for future reference. The incident as well as response should be reported to the Information Security Officer at Headquarters for further action. Formal disciplinary action would be taken against employees who have violated organizational security policies and procedures.

3.2 Security InstructionsTraining in New Systems: Training is to be provided to users and technical staff in the functionality and operations of all new systems to ensure that their use is both efficient and does not compromise Information security Acceptable Use Policy: All users must comply with the acceptable use policy for IT Resources. (Refer Acceptable Use Policy in Part-II of this document) Defending against Hackers, Stealth and Techno-Vandalism: Risks to the organisation's systems and information are to be minimized by fostering staff awareness, encouraging staff vigilance, and deploying appropriate protective systems and devices. Reporting security incidents, security weaknesses and malfunctions: All employees are encouraged to report such incidences to the Group officer in charge of the IT Application. Offices should follow a formal incident response mechanism. Responding to Virus Incidents: The threat posed by the infiltration of a virus is high, as is the risk to the organisation's systems and data files. Formal procedures for responding to a virus incident are to be developed, tested and implemented. Virus Incident response must be regularly reviewed and tested. The incident response could be along the following lines: In the case of a virus attack i. The network share of the machine has to be stopped ii. The contact person (within the office, EDP Cell) for cleaning the machine of virus has to be notified. iii. There must be a mechanism where an authorised expert/work station is notified automatically in case of a virus attack. The notified expert should perform the following action on the infected work station. i. Determine the type of virus ii. Isolate all infected systems and floppy disks. iii. Try to clean the infected file. In case of failure, the file should be deleted from the work station. iv. In case of failure above the work station should be removed from the network and remedial action taken. v. Remedial action may include reformatting depending on the severity of the problem.Delivering Awareness Programmes to Permanent Staff: Permanent staff is to be provided with Information Security awareness tools to enhance awareness and educate them regarding the range of threats and the appropriate safeguards. Information Security Officer: Training: Periodic training for the Information Security Officer is to be prioritized to educate and train on the latest threats and information security techniques. User: Information Security Training: Individual training in Information Security is mandatory, with any technical training being appropriate to the responsibilities of the user's job function. Where staff change jobs, their Information Security needs must be re-assessed and any new training provided as a priority. Technical Staff: Information Security Training: Training in Information Security threats and safeguards is mandatory, with the extent of technical training to reflect the job holder's individual responsibility for configuring and maintaining Information Security safeguards. Where IT staff change jobs, their Information Security needs must be re-assessed and any new training provided as a priority. Training New Recruits in Information security: All new staff is to receive mandatory Information Security awareness training as part of induction. Misuse of Organisation Stationery: The organization's letter-headed notepaper, printed forms and other documents are to be handled securely to avoid misuse. Third party Contractor: Awareness programmes: An appropriate summary of the Information Security Policies must be formally delivered to any such contractor, prior to any supply of services. Using Non Disclosure Agreements (Third Party): Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed to third party organisations(software developers, Maintenance vendors) is classified as Restricted (or above) Lending Keys to secure Areas to Others: The lending of keys, both physical and electronic, is prohibited. Responding to Telephone Enquiries: Telephone enquiries for sensitive or confidential information are initially to be referred to management. Only authorized persons may disclose information classified above 'Unclassified', and then only to persons whose identity and validity to receive such information has been confirmed. Reporting Information Security Incidents: All suspected Information Security incidents must be reported promptly to the designated IT Security Manager of the Office, and in critical cases, further reported to the Department's Information Security Officer. Reporting IS Incidents to outside Authorities: Information Security incidents must be reported to outside authorities whenever this is required to comply with legal requirements or regulations. This may only be done by authorized persons, and with the prior approval of the Information Security Officer at Headquarters.Reporting Information Security breaches: Any Information Security breaches must be reported without any delay to the Information Security Manager(Locally) to speed the identification of any damage caused, any restoration and repair and to facilitate the gathering of any associated evidence Notifying Information Security Weaknesses: All identified or suspected Information Security weaknesses are to be notified immediately to the Information Security Manager(Locally) Witnessing an Information Security Breach: Persons witnessing information Security incidents or breaches should report them to the Information security Manager (Locally) without delay. Being alert for Fraudulent Activities: Employees are expected to remain vigilant for possible fraudulent activities. Establishing Remedies to Information Security Breaches: A database of Information Security threats and `remedies' should be created and maintained. The database should be studied regularly with the anecdotal evidence used to help reduce the risk and frequency of Information Security incidents in the organisation.

4. Physical and Environmental Security

4.1 Guiding PrinciplesSecure Areas Objective: To prevent unauthorized access, damage and interference to business premises and information. Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference. The protection provided should be commensurate with the identified risks. A clear desk and clear screen policy is recommended to reduce the risk of unauthorized access or damage to papers, media and information processing facilities.

Equipment SecurityObjective: To prevent loss, damage or compromise of assets and interruption to business activities. Equipment should be physically protected from security threats and environmental hazards. Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

General ControlsObjective: To prevent compromise or theft of information and information processing facilities. Information and information processing facilities should be protected from disclosure to modification of or theft by unauthorized persons, and controls should be in place to minimize loss or damage.

GeneralAn important component of IT security is the integrity of the physical perimeter and facilities that contain IT resources. Access to specific areas and rooms that contain IT equipment should be restricted. This would particularly apply to rooms housing the servers. Group Officers and other senior officers must frequently visit the computer room facility on an unannounced basis during a non-prime shift and determine that access control procedures are being followed.

4.2 Security Instructions Supplying Continuous Power to Critical Equipment: An Uninterruptible Power Supply is to be installed to computing resource to ensure the continuity of services during power outages or to allow time for the orderly shutdown of systems for prolonged power outages.Managing and Maintaining Backup Power Generators: Secondary and backup power generators are to be employed where necessary to ensure the continuity of services during power outages. This would cover all applications where a downtime of over one hour is not acceptable, typically, centralized applications with over 20 computers linked to it. Using Centralised, Networked or Stand-Alone Printers: Information classified as Highly Confidential or Top Secret, may never be sent to a network printer without there being an authorised person to safeguard its confidentiality during and after printing. Installing and Maintaining Network Cabling: Network cabling should be installed and maintained by qualified engineers to ensure the integrity of both the cabling and the wall mounted sockets. Any unused network wall sockets should be sealed-off and their status formally noted. Using Lockable Storage Cupboards: Sensitive or valuable material and equipment must be stored securely and according to the classification status of the information being stored. A lockable storage cupboard should be used for storing sensitive or valuable equipment.Using Fire Protected Storage Cabinets: Documents are to be stored in a secure manner in accordance with their classification status. Backup tapes/media, User Manuals, Licensed software should be kept in Fire protected storage cabinets. Disposing of Obsolete Equipment: Equipment owned by the Indian Audit and Accounts Department may only be disposed of by authorised personnel who have ensured that the relevant security risks have been mitigated, and necessary approval from Head office obtained. The safeguards to be implemented are: Ensure that information is unrecoverable before allowing disposal of equipment. (The delete feature on most software packages is not sufficient to cleanse equipment. Deleted information may still be recoverable.) Implement procedures to destroy defective or damaged media containing sensitive information before allowing the re-use or disposal of equipment. Media may include: i. Floppy disks ii. Compact disks iii. TapesClear Screen Policy: All users of workstations, PCs / laptops are to ensure that their screens are clear / blank when not being used. This may be ensured either by closing the application, or using screen saver utility of the operating system. Clear Desk Policy: To the extent possible, the department expects all employees to operate a clear desk policy. Logon and Logoff from your Computer: Approved login procedures must be strictly observed (specific to each IT Application) and users leaving their screen unattended must firstly lock access to their workstation or log off.Taking Equipment off the Premises: Only authorised personnel are permitted to take equipment belonging to the Department off the premises; they are responsible for its security at all times. Written permission must be obtained from the Head of the Office / designated IT Security Manager of the office, and consistent with any instructions from Head office in this regard. Maintaining Hardware (On-site or Off-site Support): All equipment owned by the Department must be supported by appropriate maintenance facilities from qualified engineers. Annual Maintenance Contract should be entered into with qualified firms without fail. Recording and Reporting Hardware Faults: All information system hardware faults are to be reported promptly to the appropriate trained staff or maintenance firms and recorded in a hardware fault register maintained electronically. The rectification action taken including response time should also be noted in the inventory application, and used to assess the quality of the hardware and the firm providing maintenance support. Fire Risks to Information: All data and information must be protected against the risk of fire damage at all times. The level of such protection must always reflect the risk of fire and the value and classification of the information being safeguarded. Preparing Premises to Site Computers and related electronic equipments and ensuring environmental conditions: The sites chosen to locate computers and to store data must be suitably protected from physical intrusion, theft, and environmental threats of fire, flood and excessive ambient temperature / humidity. Physical Access Control to Secure Areas: All computer premises must be protected from unauthorised access using an appropriate balance between simple ID cards to more complex technologies to identify, authenticate and monitor all access attempts. Special instructions for Server rooms: Servers hosting critical IT Applications should be housed in a separate server room, with access to the room severely restricted to authorised personnel only. Challenging Strangers at the premises: All employees are to be aware of the need to challenge strangers on the organization’s premises. Managing On-Site and Remote Data Stores: On-site and remote locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level.Cabling Security: The security of network cabling must be reviewed during any upgrades or changes to hardware or premises.

5. Communications and Operations management 5.1 Guiding PrinciplesOperational procedures and responsibilities. Objective: To ensure the correct and secure operation of Information Processing facilities. Responsibilities and procedures for the management and operations of all information processing facilities should be established. This includes the development of appropriate operating instructions and incident response procedures. Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

System planning and acceptanceObjective: To minimize the risk of systems failure Advance planning and preparation are required to ensure the availability of adequate capacity and resources. Projections of future capacity requirements should be made, to reduce the risk of system overload. The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use.

Protection against malicious softwareObjective: To protect the integrity of software and information. Precautions are required to prevent and detect the introduction of malicious software. Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses and logic bombs. Users should be made aware of the dangers of unauthorized or malicious software, and managers should, where appropriate, introduce special controls to detect or prevent its introduction. In particular, it is essential that precautions be taken to detect and prevent computer viruses on personal computers.

HousekeepingObjective: To maintain the integrity and availability of information processing and communications services. Routine procedures should be established for carrying out agreed back-up strategy, taking backup copies of data and rehearsing their timely restoration, logging events and faults, and where appropriate, monitoring the equipment environment. Operational staff should maintain a log of their activities. Similarly, faults reported by users regarding information processing or communications systems should be logged.

Network managementObjective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure. The security management of networks which may span organizational boundaries requires attention. Additional control may also be required to protect sensitive data passing over public networks.

Media handling and securityObjective: To prevent damage to assets and interruptions to business activities. Media should be controlled and physically protected. Appropriate operating procedures should be established to protect documents, computer media (tapes, disks, cassettes), input/output data and system documentation from damage, theft and unauthorized access.

Exchanges of information and softwareObjective: To prevent loss, modification of information exchanged between organizations. Exchanges of information and software between organizations should be controlled, and should be compliant with any relevant legislation. Exchanges should be carried out on the basis of agreements. Procedures and standards to protect information and media in transit should be established. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls should be considered.

5.2 Security Instructions Using Fax Machines / Fax Modems: Sensitive or confidential information may only be faxed where more secure methods of transmission (encrypted, digitally signed e-mail) are not feasible. Both the owner of the information and the intended recipient must authorize the transmissions beforehandUsing Modems / ISDN / DSL connections: Sensitive or confidential information may only be sent via public telephone lines where more secure methods of transmission are not feasible. Both the owner of the information and the recipient must authorize the transmission beforehand. Controlling IT consumables: IT Consumables must be purchased in accordance with the Organization's approved purchasing procedures with usage monitored to discourage theft and improper use. Using Removable Storage Media including Diskettes and CDs: Only personnel who are authorised to install or modify software shall use removable media to transfer data to / from the organisation's network. Any other persons shall require specific authorisation. Specific authorisation would also be required for sending organisational data over removable media by post. Receiving Information on Disks: The use of removable media disks e.g. disks, CD-ROMs and USB Memory sticks is not permitted on critical information system Networks except where specifically authorized by the System Administrator of the network/Group Officer in charge. Damage to Equipment: Deliberate or accidental damage to organisation property must be reported to the nominated IT Security Manager (local) and if critical, Information Security Officer, at Head office as soon as it is noticed.Defending the Network Information from Malicious Attack: System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised network intrusion. Managing System Operations and System Administration: The organisation's systems must be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the organisation’s information security. Managing System Documentation: System documentation is a requirement for all the organisation’s information systems. Such documentation must be kept up-to-date and be available. Monitoring Operational Audit Logs: Operational audit logs are to be reviewed regularly by the designated system administrator and discrepancies reported to the owner of the information system.Responding to System Faults: Only qualified and authorised staff or approved third party technicians/AMC service providers may repair information system hardware faults. Downloading Files and Information from the Internet: Great care must be taken when downloading information and files from the Internet to safeguard against both malicious code and also inappropriate material. (for details, refer Acceptable use Policy) Sending Electronic Mail (E-mail): E-mail should only be used for business purposes, using terms which are consistent with other forms of business communication. The attachment of data files to an e-mail is only permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code. (for details, refer e-mail Policy) Receiving Electronic Mail (E-mail): Incoming e-mail must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code. (for details, refer e-mail Policy) Using Internet ‘Search Engines’: Information obtained from Internet sources should be verified before used for business purposes. The trustworthiness of the site, Authentication etc should be given due weightage while assessing the quality and reliability of information. Developing a Web Site: Due to the significant risk of malicious intrusion from unauthorized external persons, as well as dissemination of unauthorized information, Web sites may only be developed and maintained by properly qualified and authorised personnel, and after prior approval of the Functional/IT wing of Headquarters. Preference may be given to outsource the web hosting service to vendors of repute, with documented Service Level Agreement. Maintaining Web Sites: The Web site is an important information resource for the organisation, and its safety from unauthorised intrusion is a top priority. Only qualified authorised persons may amend the Web site with all changes being documented and reviewed. The website should accordingly be hosted with a reputed ISP (Internet Service Provider) after obtaining necessary assurance of their ability to protect the organisation’s website from external hacking attacks. The Information on the Web site must be kept up to date, and the content periodically reviewed for accuracy and contemporariness. Certainty of File Origin: Computer files received from unknown senders are to be deleted without being opened. Receiving Misdirected Information by Fax: Any fax received in error is to be returned to the sender. Its contents must not be disclosed to other parties without the sender's permission. Persons Giving Instructions over the Telephone: The identity of recipients of sensitive or confidential information over the telephone must be verified. Persons Requesting Information over the Telephone: The identity of persons requesting sensitive or confidential information over the telephone must be verified, and they must be authorised to receive it. Transferring and Exchanging Data: Sensitive or confidential data / information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured e.g. by using encryption techniques. Managing Data Storage: Day-to-day data storage must ensure that current data is readily available to authorised users and that archives are both created and accessible in case of need. Setting up New Databases: Databases must be fully tested for business logic and processing, prior to operational usage. The reports of such testing are to be retained for subsequent inspection. Restarting or Recovering your System: Information system owners must ensure that adequate back up and system recovery procedures are in place. Managing Backup and Recovery Procedures: Backup of the organisation's data files and the ability to recover such data is a top priority. Management is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business, and are consistent with the prescribed backup and Recovery procedure for the IT Application. Archiving Information: The storage media used for the archiving of information must be appropriate to its expected longevity. Recovery and Restoring of Data Files: Management must ensure that safeguards are in place to protect the integrity of data files during the recovery and restoration of data files; especially where such files may replace more recent files. Managing Hard Copy Printouts: Hard copies of sensitive or classified material must be protected and handled according to the distribution and authorisation levels specified for those documents. Photocopying Confidential Information: All employees are to be aware of the risk of breaching confidentiality associated with the photocopying (duplication) of sensitive documents. Authorisation from the document owner should be obtained where documents are classified as Highly Confidential or above. Filing of Documents and Information: All information used for, or by the organisation, must be filed appropriately and according to its classification. Shredding of Unwanted Hardcopy: All documents of a sensitive or confidential nature are to be shredded when no longer required. The document owner must authorise or initiate this destruction. Using Good Document Management Practice: All users of information systems must manage the creation, storage, amendment, copying and deletion / destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. The degree to which software techniques and disciplined user procedures are necessary will be applied by management and determined by the classification of the information / data in question. Need for Dual Control / Segregation of Duties: The techniques of dual control and segregation of duties are to be employed to enhance the control over procedures wherever both the risk from, and consequential impact of, a related Information Security incident is likely to be critical. Recording and Reporting Software Faults: Software faults are to be formally recorded and reported to those responsible for software support / maintenance, typically, the EDP Cell in each office. Software Development: Software developed for or by the organisation must always follow a formalised development process which itself is managed under the project in question. The integrity of the organisation's operational software code must be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures. Separating Systems Development and Operations: Management must ensure that proper segregation of duties applies to all areas dealing with systems development, systems operations, or systems administration. Capacity Planning and Testing of New Systems: New systems must be tested for capacity, peak loading and stress testing. They must demonstrate a level of performance and resilience which meets or exceeds the technical and business needs and requirements of the organisation. Documenting New and Enhanced Systems: All new and enhanced systems must be fully supported at all times by comprehensive and up to date documentation. New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available. Defending Against Virus Attacks: Without exception, Anti Virus software is to be deployed across all PCs with regular virus definition updates and scanning across servers, PCs and laptop computers. Installing Virus Scanning Software: Anti Virus software must be chosen from a proven leading supplier. Investigating the cause and Impact of IS Incidents: Information Security incidents must be properly investigated by suitably trained and qualified personnel. Collecting Evidence of an Information Security Breach: Evidence relating to an Information Security breach must be properly collected and forwarded to the Information Security Officer. Ensuring the Integrity of IS Incident Investigations: The use of information systems must be monitored regularly with all unexpected events recorded and investigated. Such systems must also be periodically audited with the combined results and history strengthening the integrity of any subsequent investigations. Analyzing IS Incidents Resulting from System Failures: Information Security incidents arising from system failures are to be investigated by competent technicians. Breach in Confidentiality: Breaches of confidentiality must be reported to the Information Security Officer as soon as possible. Monitoring Confidentiality of Information Security Incidents: Information relating to Information Security incidents may only be released by authorized persons after seeking approval of the Information Security Officer. Maintaining confidentiality of Information Security incidents whilst they are being investigated is important for the reputation of the organisation. Monitoring Error Logs: Error logs are the reports produced by the system relating to errors or inconsistencies that have arisen during processing and are important sources of information for ensuring proper use of the system. Error logs must be properly reviewed and managed by the designated system administrator.

6. Access Control6.1 Guiding Principles Business requirements for access control Objective: To control access to information. Access to information, and business processes should be controlled on the basis of business and security requirements. This should take account of policies for information dissemination and authorization.

User access managementObjective: To prevent unauthorized access to information systems. Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedure should cover all stages in the life cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

User responsibilitiesObjective: To prevent unauthorized user access. The co-operation of authorized users is essential for effective security. Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of password and the security of user equipment.

Network access controlObjective: Protection of networked services Access to both internal and external networked services should be controlled. This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services by ensuring: Appropriate interfaces between the organization’s network and networks owned by other organizations, or public networks. Appropriate authentication mechanisms for users and equipment; Control of user access to information services.

Operating system access controlObjective: To prevent unauthorized computer access. Security facilities at the operating system level should be used to restrict access to computer resources. These facilities should be capable of the following: Identifying and verifying the identity, and if necessary the terminal or location of each authorized users. Recording successful and failed system accesses. Providing appropriate means for authentication; if a password management system is used, it should ensure quality passwords Where appropriate, restricting connection time of users. Application access controlObjective: To prevent unauthorized access to information held in information systems. Logical access to software and information should be restricted to authorized users. Application systems should: Control user access to information and application system functions, in accordance with a defined business access control policy. Provide protection from unauthorized access for any utility and operating system software that is capable of overriding system or application controls. Not compromise the security of other systems with which information resources are shared. Be able to provide access to information to the owner only, other nominated authorized individuals, or defined group of users.

Monitoring system access and useObjective: To detect unauthorized activities Systems should be monitored to detect deviation from access control policy and record monitorable events to provide evidence in case of security incidents. System monitoring allows the effectiveness of control adopted to be checked and conformity to an access policy model to be verified.

Mobile computing and teleworkingObjective: To ensure security when using mobile computing and teleworking facilities. The protection required should be commensurate with the risks their specific way of working cause. When using mobile computing, the risks of working in an unprotected environment should be considered and appropriate protection applied.

6.2 Security Instructions Managing Access Control Standards: Access control standards for information systems must be established by the Head of the office and should incorporate the need to balance restrictions to prevent unauthorized access against the need to provide unhindered access to meet business needs. The Access Control standards should be translated into an Access Control Document, listing out the level of privilege for each authorized category of user in the office. This should be in keeping with the guidelines on access control for each of the large IT Applications of Indian Audit and Accounts Department(Under preparation). Managing User Access: Access to all systems must be authorised by the owner of the system (Group Officer in charge of the function) and such access, including the appropriate access rights (or privileges) must be recorded in an Access Control List. The Access Control list may be in the form of a register maintained manually or electronically. A formal review of user's access rights should be conducted by the Security Manager such that: User's access rights are reviewed at least once in 6 months and after any change Authorisation for special privileged access rights are reviewed once in 3 months. Privileged allocations are checked at regular intervals(at least once in 3 months) to ensure that unauthorised privileges have not been obtained. Managing Network Access Controls: Access to the resources on the network must be strictly controlled to prevent unauthorised access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised. Controlling Access to Operating System Software: Access to operating system commands is to be restricted to those persons who are authorised to perform systems administration / management functions. Even then, such access must be operated under dual control requiring the specific approval of senior management/Group officer in Charge. Managing Passwords: The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to the Password Policy. In particular, passwords shall not be shared with any other person for any reason. Securing Against Unauthorised Physical Access: Physical access to high security areas is to be controlled with strong identification and authentication techniques. Staff with authorisation to enter such areas is to be provided with information on the potential security risks involved. Monitoring System Access and Use: Access to critical application components is to be logged and monitored to identify potential misuse of systems or information. In case of database related application, audit trails are to be enabled for all sensitive data access, and reviewed on a fortnightly basis. Giving Access to Files and Documents: Access to information and documents is to be carefully controlled, ensuring that only authorised personnel may have access to sensitive information. Managing Higher Risk System Access: Access controls for highly sensitive information or high risk systems are to be set in accordance with the value and classification of the information assets being protected. Controlling Remote User Access: Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Such access to the organisation's network and resources will only be permitted provided that authorised users are authenticated, data is encrypted across the network, and privileges are restricted. Configuring Networks: The network must be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions. Managing Network Security: Access to the resources available from the organization's network must be strictly controlled in accordance with the agreed Access Control List, which must be maintained and updated regularly. Defending Against Premeditated Cyber Crime Attacks: Security on the network accessible from outside the organization is to be maintained at the highest level. Those responsible for the network and external communications are to receive proper training in risk assessment and how to build secure systems which minimise the threats from cyber crime. Controlling Data Distribution: For authorised personnel, the appropriate data and information must be made available as and when required; for all other persons, access to such data and information is prohibited with appropriate technical control required to supplement the enforcement of this policy. Synchronizing System Clocks: System clocks must be synchronized regularly especially between the organisation's various processing platforms. In case of client-server applications, the system should take the timestamp from the Server clock. Setting up Intranet Access: While setting up Intranet access, it must be ensured that any access restrictions pertaining to the data in source systems are also applied to access from the organisation's Intranet. Setting up Extranet Access: While setting up Extranet access, it must be ensured that any access restrictions pertaining to the data in source systems are also applied to access from the organisation's Extranet. Setting up Internet Access: While setting up Internet access over a Local Area Network, it must be ensured that the organisation's network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall(Hardware or Software). Internet access (including e-mail) must be in keeping with the Acceptable use Policy and also compliant with the organisation's Information Security Policies. Filtering Inappropriate Material from the Internet: The organisation may use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by staff. Reports of attempted access will be scrutinized by management on a regular basis. Handling Staff Resignations: Upon notification of staff resignations, Human Resources management must consider with the Information Security Manager (Locally) whether the member of staff's continued system access rights constitutes an unacceptable risk to the Office and, if so, revoke all access rights. Limit connection times: Timed logins are to be used to protect critical applications and data that require added security. Timed logins allow specific users to access the system at specific times. Security administrators and business management should be consulted before overriding any timed login. Establish session time-outs: Each application should provide for session time-outs that will terminate a connection that has been inactive for a certain period of time. The length of time before time-out should be determined by: · Level of risk associated with a logged in session· Sensitivity of dataDefending Against Premeditated Internal Attacks: In order to reduce the incidence and possibility of internal attacks, access control standards and data classification standards are to be periodically reviewed whilst maintained at all times. Issuing Laptop / Portable Computers to Personnel: Management must authorise the issue of portable computers. Usage is to be restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devicesDay to Day Use of Laptop / Portable Computers: Laptop computers are to be issued to, and used only by, authorized employees and only for the purpose for which they are issued.Persons who are issued with portable computers and who intend to travel for business purposes must be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimise the risks. The IS issues relevant to Mobile computing are: disclosure of confidential data on laptop, virus threats, theft. It is the responsibility of the user of the Laptop to ensure that has suitable antivirus and encryption software installed on it, and that the anti-virus is updated regularly. Care should be taken in the handling of laptop to avoid loss due to theft and damage. Backing up Data on Portable Computers: Information and data stored on Laptop or portable computers must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis. Respecting Privacy and Confidentiality of information: Information related to Entitlement function of the organisation covering Provident Fund balance, retirement benefits etc. of State Government employees are inherently confidential. Employees authorised access to this information should not disclose it to unauthorised personnel, both within and outside the office. Appropriate access control methods should be instituted while allowing access to such information over IVRS/Website.

7. System development and maintenance 7.1 Guiding PrinciplesSecurity requirement of systems Objective: To ensure that security is built into information systemsThis will include infrastructure, business applications, and user developed applications. The design and implementation of the business process supporting the application or service can be crucial for security. Security requirements should be identified and agreed prior to the development of information systems. All security requirements, including the need for fallback arrangements, should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system. The framework for analyzing security requirements and identifying controls to fulfil them is risk assessment and risk management.

Security in application systemObjective: To prevent loss, modification or misuse of user data in application systems. Appropriate controls and audit trails or activity logs should be designed into application systems, including user written applications. These should include the validation of input data, internal processing and output data.

Cryptographic controlsObjective: To protect the confidentiality, authenticity or integrity of information. Cryptographic systems and techniques should be used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

Security of System filesObjective: To ensure that IT Projects and support activities are conducted in a secure manner. Access to system files should be controlled. Maintaining system integrity should be the responsibility of the user function or development group to whom the application system or software belongs.

Security in development and support processes.Objective: To maintain the security of application system software and information. Project and support environment should be strictly controlled. Managers responsible for application development should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment. 7.2 Security Instructions

Managing or Using Transaction / Processing Reports: Transaction and processing reports should be regularly reviewed by properly trained and qualified staff. These reports, to be produced at the desired intervals, would show the entries processed for the period in question. Such reports should be either printed automatically, or be available 'on line'.Using and Receiving Digital Signatures: The transmission of sensitive and confidential data is to be authenticated by the use of digital signatures whenever possible. Managing Databases: The integrity and stability of the organisation’s databases must be maintained at all times. Permitting Emergency Data Amendment: Emergency data amendments, bypassing the normal controls, may only be used in extreme circumstances and only after approval of the Group Officer in Charge of the IT Application. Making Emergency Amendments to Software: Emergency amendments to software are to be discouraged, except in circumstances designated by management as 'critical'. Any such amendments must strictly follow agreed change control procedures. Using Version Control Systems: Version control procedures should always be applied to documentation belonging to the organization. Using Encryption Techniques: Where appropriate, sensitive or confidential information or data should always be transmitted in encrypted form. Applying ‘Patches’ to Software: Patches to resolve software bugs may only be applied where verified as necessary and with management authorisation. Operating System Software Upgrades: Necessary upgrades to the Operating System of any of the organization’s computer systems must have the associated risks identified and be carefully planned, incorporating tested fall-back procedures. All such upgrades must be undertaken as a formal project. Restriction on changes to software package: Modifications to software packages is strongly discouraged. As far as possible, and practicable, vendor-supplied software packages should be used without modificationManaging Operational Program Libraries/Program Source Libraries: Only designated staff may access operational program libraries/program source libraries. Amendments may only be made using a combination of technical access controls and robust procedures operated under dual control. Managing Change Control Procedures: Formal change control procedures must be utilized for all amendments to systems. All changes to programs must be properly authorized and tested in a test environment before moving to the live environment. The Change control Procedure should encompass the following:Maintaining a record of agreed authorization levels Ensuring changes are submitted by authorized users Reviewing controls and integrity procedures to ensure that they will not be compromised by changes Identifying all computer software, information, database entities and hardware that require amendment. Obtaining formal approval for detailed proposals before work commences. Ensuring that the authorized user accepts changes prior to any implementation. Ensuring that implementation is carried out to minimize business disruptions Ensuring that system documentation set is updated on the completion of each change that old documentation is archived or disposed of Maintaining a version control for all software updates Maintaining an audit trail of all change requests Ensuring that operating documentation and user procedures are changed as necessary to be appropriate Ensuring that the implementation of changes takes place at the right time and is not disturbing the business process involved. Using Live Data for Testing: The use of live data for testing new system or system changes may only be permitted where adequate controls for the security of the data are in place. Parallel Running: Normal System Testing procedures will incorporate a period of parallel running prior to the new or amended system being acceptable for use in the live environment. The results of parallel running should not normally reveal problems or difficulties which were not previously passed during User Acceptance Testing. Outsourced software development: In case of outsourced software development, the issues relating to licensing arrangements, quality certification, intellectual property rights, escrow arrangements should be suitable considered. Care should be taken to ensure that the Intellectual Property Rights of the Software developed by a third party to meet the department's requirement rests with the Department.

8. Business continuity management

8.1 Guiding PrinciplesAspects of business continuity management: Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters. A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures to an acceptable level through a combination of preventative and recovery controls. Business continuity should begin with threat identification and risk assessment, with full involvement of the owners of business resources and processes. This would lead to the preparation of the strategic plan for the overall approach to business continuity. The consequences of disasters, security failures and loss of service should be analyzed. Contingency plans should be developed and implemented to ensure that business processes can be restored within the required time-scales. Such plans should be maintained and practiced to become an integral part of all other management processes. Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. The BCP should be tested regularly to ensure that they are up to date and periodically reviewed to ensure their continuing effectiveness.

A key component of the Business Continuity Plan is the backup and recovery procedure for the IT Application. Each office of Indian Audit and Accounts Department would base its Backup Procedure on the best practices guideline for Backup and Recovery issued by the IT Wing of Head Office. Deviation, if any, from the prescribed procedure should be recorded, and formal approval of IT Wing taken.The Head of the office (Accountant General/Principal Director) would be the owner of the Business Continuity Plan for each application, and would be responsible for any data loss/Business down time due to failure of the IT System, and the non availability of suitable backups to restore the system.

8.2 Security Instructions: 1. Initiating the BCP Project: The Head of the Office (Accountant General/Principal Director) is required to initiate a Business Continuity Plan. Business Continuity Planning (BCP) is essential for the continuation of key business services, in the event of an unexpected occurrence which seriously disrupts the business process.2. Assessing the BCP Security Risk: The Accountant General is to undertake a formal risk assessment in order to determine the requirements for a Business Continuity Plan.3. Developing the BCP: The Accountant General is to develop a Business Continuity Plan which covers all essential and critical business activities.4. Testing the BCP: The Business Continuity Plan is to be periodically tested to ensure that the management and staff understand how it is to be executed.5. Training and Staff Awareness on BCP: All staff must be made aware of the Business Continuity Plan and their own respective roles6. Maintaining and Updating the BCP: The Business Continuity Plan is to be kept up to date and re-tested periodically.7. Backup Procedures: Implement procedures to back-up data on a regular basis, consistent with the Guidelines issued by Head Office. The backups have to be restored at least once in two weeks and the logs of success/failure maintained.8. Backup Storage: Store back-ups at a secure, remote location. Apply the same standards to back-ups that apply to media on the main site. The backup media at local site should be kept in a fireproof safe. One copy of the backup should necessarily be stored at an offsite location. 9. Disaster Recovery Plan: Owners of the organization’s information systems must ensure that disaster recovery plans for their systems are developed, tested, and implemented. A Disaster Recovery Plan is an important preliminary part of the organization’s Business Continuity Plan (BCP). A severe incident can affect any organization at any time and all organizations should ensure that they have both a DRP and a BCP. 10. Minimising the Impact of Cyber Attacks: Plans are to be prepared, maintained and regularly tested to ensure that damage done by possible external cyber crime attacks can be minimized and that restoration takes place as quickly as possible.

9. Compliance 9.1 Guiding Principles Compliance with legal requirements Objective: To avoid breaches of any criminal and civil laws, statutory, regulatory or contractual obligations and of any security requirements. The design, operation, use and management of information security systems may be subject to statutory, regulatory and contractual security requirements. Advice on specific legal requirements should be sought from the organization’s legal advisers, or suitably qualified legal practitioners.

Reviews of security policy and technical complianceObjective: To ensure compliance of systems with organizational security policies and standards The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with security implementation standards.

9.2 Security Instructions 1. Using Licensed Software: To comply with legislation and to ensure ongoing vendor support, the terms and conditions of all End User License Agreements are to be strictly adhered to.2. Being Aware of Legal Obligations: All employees are to be fully aware of their legal responsibilities with respect to their use of computer based information systems and data. The relevant extracts of IT Act 2000 are reproduced in Appendix II-9-1.3. Complying with General Copyright Legislation: All employees are to be aware of the key aspects of Copyright, Designs and Patents Act legislation (or its equivalent), in so far as these requirements impact on their duties. The relevant provisions of the Indian

Copyright Act are explained in Appendix II-9-2.Archiving Documents: The archiving of documents/data must take place consistent with the archival policy for each data-system, which has to be prepared with due consideration for legal, regulatory and business issues with liaison between technical and business staff. Where no archiving policy exists, no data may be deleted from the system, except with the explicit approval of the IT and functional wing of Headquarters office. 5. Information Retention Policy: The information created and stored by the organisation's information systems must be retained for a minimum period that meets both legal and business requirements. Guidelines issued in this regard from Headquarters are to be scrupulously followed. Where no such guideline exists, no data may be deleted from the system, except with the explicit approval of the IT and functional wing of Headquarters office.6. Handling Draft Reports: Draft reports should be clearly labelled as such, and only be updated with the authority of the designated owner of the report. Draft version(s) of reports must be deleted or archived following production of a final version. A single version of the file should be retained for normal operational access.7. Managing Media Storage and Record Retention: Each office of the organisation will maintain a suitable archiving and record retention procedure.8. Complying with Information Security Policy: All employees are required to fully comply with the organisation's Information Security policies. The monitoring of such compliance is the responsibility of the Security Manager of the office. To ensure compliance with the Security Policy, Internal Audit would conduct an Audit of the management of IT Assets within the office, and the findings of the Audit would be communicated to the Information Security Officer after discussion with the Head of the Office and Security Manager. Any Information Security incidents resulting from non-compliance will result in immediate disciplinary action.9. Safeguarding against Libel and Slander: Employees are prohibited from writing derogatory remarks about other persons or organizations. Casual comments in e-mails relating to individuals or other organisations may be construed as defamatory - even if the comments are valid.10. Using copyrighted Information from the Internet: Information from the Internet or other electronic sources may not be used without authorisation from the owner of the copyright.11. Sending Copyrighted Information Electronically: Information from the Internet or other electronic sources may not be retransmitted (e-mail and web based links) without permission from the owner of the copyright. 12. Using Text directly from Reports, Books or Documents: Text from reports, books or documents may not be reproduced or reused without permission from the copyright owner.13. Recording Evidence of Incidents (Information Security): The Security Manager of the office is to be aware that evidence of Information Security incidents must be formally recorded and retained and passed to the Information Security Officer at the Head Office in all cases of Information Security incidents involving outside parties.14. Respecting Privacy in the Workplace: Notwithstanding the organization’s respect for employee's privacy in the workplace, it reserves the right to have access to all information created and stored on the organization’s systems.15. Sharing employee Information with Other Employees: Employee data may only be released to persons specifically authorized to receive this information.16. Handling Confidential Employee Information: All employee data is to be treated as strictly confidential and made available to only properly authorized persons.17. Using the Internet in an Acceptable Way: Employees may not use the organization’s systems to access or download material from the Internet which is inappropriate, offensive, illegal, or which jeopardizes security. Internet use must be primarily for business related purposes, and consistent with the Acceptable use policy of the Department.18. Keeping Passwords / PIN Numbers Confidential: All personnel must treat passwords as private and highly confidential. Non-compliance with this policy could result in disciplinary action.19. Using E-Mail and Postal Mail Facilities for Personal Reasons: The use of e-mail for personal use is discouraged, and should be kept to a minimum. Postal mail may be used for business purposes only.20. Playing Games on Office Computers: The playing of games on office PCs or laptop is prohibited.21. Using Office Computers for Personal Use: Using the organization's computers for personal / private business is strongly discouraged. Limited use in keeping with the Acceptable use policy is permitted.22. Compliance with Access Controls: All employees will use the IT applications with the privileges assigned to them in keeping with the Access Control guidelines for the application. Attempts at subverting the access controls, or disclosing privileged information to unauthorised individuals would invite disciplinary action.23. Compliance with Information Classification restrictions: All Employees should comply with the instructions relating to information classification. Specifically, employees with access to information of a higher level of sensitivity may not divulge it to employees who do not have such access.

Appendix II-9-1 (IT Act 2000: Relevant Extracts)Important Provisions of IT Act 2000 which should be known by all employees of Indian Audit and Accounts Department.

Authentication of electronic records:(Clause 3) (1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature. (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.(3) Any person by the use of a public key of the subscriber can verify the electronic record. (4) The private key and the public key are unique to the subscriber and constitute a functioning key pair. Legal recognition of electronic records.(Clause 4): Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is— (a) rendered or made available in an electronic form; and (b) accessible so as to be usable for a subsequent reference.Legal recognition of digital signatures:(Clause 5): Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (hen, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.Use of electronic records and digital signatures in Government and its agencies: (Clause 6): (1) Where any law provides for- o (a) the filing of any form. application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;o (b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;o (c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government. (2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe-o (a) the manner and format in which such electronic records shall be filed, created or issued;o (b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause Retention of electronic records: (Clause 7): (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if-o (a) the information contained therein remains accessible so as to be usable for a subsequent reference;o (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;o (c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record: Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received. (2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Sections 6,7 and 8 not to confer right to insist document should be accepted in electronic form: (Clause 9): Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form Penalty for damage to computer, computer system, etc. (Clause 43): If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, (a) accesses or secures access to such computer, computer system or computer network; (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; (e) disrupts or causes disruption of any computer, computer system or computer network; (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder; (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. Tampering with computer source documents.(Clause 65): Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. Explanation.—For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and Programme analysis of computer resource in any form. Hacking with computer system(Clause 66): · (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:· (2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.Publishing of information which is obscene in electronic form.(Clause 67): Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees. Protected system(Clause 70) (1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. (2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1). (3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.Penalty for breach of confidentiality and privacy. (Clause 72): Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Appendix II-9-2 (Indian Copyright Act: Relevant Extracts) Extracts from the Indian Copyright Act to be known by all employees of Indian Audit and Accounts Department The Indian Copyright Act was amended in 1994 to extend more effective protection to computer programmes as literary works and for the protection of computer generated works. The meaning of “literary work” included works such as computer programmes, tables and compilations including computer databases. The rights of the copyright holder, the rights of the users, and the punishment on infringement of copyright of software etc., are all extensively covered. India being part of Bern convention (1971) the Rome Convention, Indian Copyright Act as amended in 1994 with broad-based definition of software and making copyright infringement as a cognizable offence is rated as one of the effective pieces of legislation. Major changes to Indian Copyright Law introduced in 1994 and came into effect from 10 May 1995. According to this Act, the infringer can be tried under both civil and criminal law.

According to section 14 of this Act, it is illegal to make or distribute copies of copyrighted software without proper or specific authorisation. The only exception is provided by section 52 of the Act, which allows a backup copy purely as a temporary protection against loss, distribution or damage to the original copy. The 1994 amendment to the Copyright Act also prohibits the sale or hiring, or any offer for sale or hire of any copy of the computer program without specific authorisation of the Copyright holder.

A civil and criminal action may be instituted for injunction, actual damages (including infringer's profits) or statutory damages per infringement etc. With these amendments, even the criminal penalties have substantially increased. Section 63 B, stipulates a minimum jail term of 7 days which can be extended up to 3 years. The Act further states the fine ranging from Rs. 50,000 to 2,000,000.

1. Information Technology Acceptable Use Policy

1.0 Overview

The intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to IAAD’s established culture of trust and integrity. IAAD is committed to protecting its employees, and the Department from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of IAAD. These systems are to be used for business purposes in serving the interests of the organization. Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at IAAD. These rules are in place to protect the employee and the department. Inappropriate use exposes IAAD to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Indian Audit and Accounts Department, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by IAAD.

4.0 Policy

4.1 General Use and Ownership

While it is our desire to provide a reasonable level of privacy, users should be aware that the data they create on the organisation’s systems remains the property of the Department. Because of the need to protect IAAD's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the Department.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. The criteria of misuse of Government resources should govern the action of the employees. If there is any uncertainty, employees should consult their supervisor or manager.

It is recommended that any information that users consider sensitive or vulnerable be encrypted.

For security and network maintenance purposes, individuals authorized by Information Security Officer within IAAD may monitor equipment, systems and network traffic at any time.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as per the classification guidelines (Unclassified, Operational Use Only, Private, Restricted, Confidential), and suitable access controls built accordingly. Employees should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months. **3.** All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended. **4.** Use encryption of information in keeping with the sensitivity of the data. **5.** Because information contained on portable computers is especially vulnerable, special care should be exercised. Confidential Data contained in Laptops should be kept encrypted. **6.** Postings by employees from an IAAD email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of IAAD, unless posting is in the course of business duties. The user of official e-mail ID should normally be avoided in such newsgroup postings. **7.** All hosts used by the employee that are connected to the Department's Internet/Intranet/Extranet, whether owned by the employee or Department shall be continually executing approved virus-scanning software with a current virus database. **8.** Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of IAAD authorized to engage in any activity that is illegal under Union, State, or international law while utilizing IAAD owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions: **1**Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by IAAD. **2** Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which IAAD or the end user does not have an active license is strictly prohibited. **3**Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.). **4** Installation of any freeware/Shareware software, including computer games on IAAD owned computing resource without approval of the Information Security Manager of the office **5**Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home. **6** Using an IAAD computing asset to actively engage in procuring or transmitting material that may be construed as sexual harassment or leading to hostile workplace environment. **7** Making fraudulent offers of products, items, or services originating from any IAAD account. **8** Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes. **9** Port scanning or security scanning is expressly prohibited unless prior notification to Information Security Officer is made. **10** Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty. **11** Circumventing user authentication or security of any host, network or account. **12** Interfering with or denying service to any user other than the employee's host (for example, denial of service attack). **13**Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Email and Communications Activities

1Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). **2** Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages. **3** Unauthorized use, or forging, of email header information. **4**Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies. **5** Creating or forwarding "chain letters". **6** Posting non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Use of Internet

1.Internet access using Departmental resources should be properly used. You shall not violate any law, interfere with network users, services, or equipment, or harass other users. **2.**Personal Internet use is authorized; however, employees may use the Internet on a limited basis as long as it does not disrupt operations, detract from other tasks, or otherwise violate departmental or state policy. **3.** It is to be noted that copyrighted material may not be duplicated or used in any manner that infringes on the copyright. **4.** Downloading and uploading of software that is protected by a license agreement may only be done in strict compliance with the license agreement and applicable state policy. **5.** Be aware that freeware programs may not be free for business use. Be sure to follow any and all licensing agreements thoroughly. Prior to downloading software, obtain clearance and approval for use from the designated Information Security Manager, who may refer the case to the Information Security Officer in case of any doubt.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

6.0 Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.

2. Email Policy

1.0 Overview

Email is a quick, cheap and easy means of communication. This makes email a great business tool, but at the same time a potential threat for employers. Email threats such as confidentiality breaches, legal liability, lost productivity and damage to reputation cost organisations substantial amount each year. E-mail usage has become a standard feature of our department, and it is necessary that all employees comply with the best practices identified in this guideline.

2.0 Purpose

The purpose of this policy is to establish a standard for use of e-mail in Indian Audit and Accounts Department.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an e-mail account on any system that resides at any IAAD facility, or has an account with the IAAD mail-server under the CAG’s domain. (@cag.gov.in)

4.0 Policy

IAAD considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in increasing productivity. Users should take the same care in drafting an email as they would for any other communication. Therefore IAAD wishes users to adhere to the following guidelines: • Writing emails: **o** Write well-structured emails and use short, descriptive subjects. **o** Signatures must include your name, designation and office name. A disclaimer will be added underneath your signature (see Disclaimer). **o** Users must spell check all mails prior to transmission. **o** Do not send unnecessary attachments. Compress attachments larger than 200K before sending them. **o** Do not write emails in capitals. **o** Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware that you will be copying a mail to him/her and knows what action, if any, to take. **o** If you forward mails, state clearly what action you expect the recipient to take. **o** Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, encrypting the mail using S/MIME or PGP, or using other means of communication, or protecting information by using a password. **o** Only mark emails as important if they really are important. · Replying to emails: **o** Emails should be answered preferably by e-mail. · Newsgroups: **o** Officials may not subscribe to a newsletter or news group using the official e-mail account(@cag.gov.in e-mail ids). · Maintenance: **o** Delete any email messages that you do not need to have a copy of, and set your email client to automatically empty your 'deleted items' on closing. Personal Use It is strictly prohibited[C1] to use IAAD's email system, using the official e-mail id (xyz@cag.gov.in) for anything other than legitimate business purposes. Therefore, the sending of personal emails, chain letters, junk mail, jokes and executables is disallowed. All messages distributed via the Department's email system are IAAD's property. Confidential information Never send any confidential information via email unless it is encrypted with S/MIME / PGP and digitally signed. ENCRYPTION All information, which is not in Public domain, like Audit Reports at the Draft Para Stage, Finance and Appropriation accounts before tabling in the legislature etc. has to be encrypted using S/MIME / PGP before being sent by e-mail. DIGITAL SIGNATURE All official e-mails by IAAS officers/Officers at CAG's Office are to be digitally signed. Executive decisions like sanction of funds, grant of leave, posting orders etc. communicated through e-mail will not be taken cognizance of unless they bear digital signature of the competent authority / authorised sender. Email accounts All email accounts maintained on the Department's email systems are property of IAAD. Passwords should not be given to other people and should be changed once a quarter. System Monitoring Users expressly waive any right of privacy in anything they create, store, send or receive on the Department's computer system. IAAD can, but is not obliged to, monitor emails without prior notification. If there is evidence that you are not adhering to the guidelines set out in this policy, the Department reserves the right to take appropriate disciplinary action. Disclaimer The following disclaimer will be added to each outgoing email: 'This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager (system@cag.delhi.nic.in). Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the company. Finally, although the organisation has taken reasonable precautions to ensure no viruses are present in this email, the organisation cannot accept responsibility for any loss or damage arising from the use of this email or attachments.' Email Retention The email retention policy is secondary to IAAD’s extant instructions on Record Keeping. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner. All IAAD’s email information is categorized into two main classifications with retention guidelines: General Correspondence: As per corresponding prescribed retention period for the base document. The Officer to whom the mail is addressed is responsible for email retention of General Correspondence. E-mail may be destroyed after a period of 60 days, if a print of the same has been taken, and kept in the relevant file. Ephemeral Correspondence (Retain until read, destroy): This covers all informal mails exchanged between officers. This may be read and destroyed, in any case within 30 days of receipt. IAAD’s encrypted communications should be stored in a manner consistent with informational content of the e-mail, but in general, information should be stored in a decrypted format. 5.0 Enforcement Any employee found to have violated this policy may be subject to disciplinary action.

3. Password Policy 1.0 Overview Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of IAAD's network. As such, all IAAD employees (including contractors and vendors with access to IAAD systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. 2.0 Purpose The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. 3.0 Scope The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any IAAD facility, has access to the IAAD network, or stores any non-public IAAD information. 4.0 Policy 4.1 General · All system-level passwords (e.g., root, NT Admin, application administration accounts, etc.) must be changed at least on quarterly basis. Passwords for corporate e-mail accounts are also to be changed quarterly. · All user-level passwords (e.g. web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months. · User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user. · Passwords must not be inserted into email messages or other forms of electronic communication. · All user-level and system-level passwords must conform to the guidelines described below. 4.2 Guidelines A. General Password Construction Guidelines Passwords are used for various purposes at IAAD. Some of the more common uses include: user level accounts, web accounts, email accounts and screen saver protection. Since no systems currently have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords. Poor, weak passwords have the following characteristics: · The password contains less than eight characters · The password is a word found in a dictionary (English or foreign) · The password is a common usage word such as: o Names of family, pets, friends, co-workers, fantasy characters, etc. o Computer terms and names, commands, sites, companies, hardware, software. o The words "IAAD", "AGAUDIT", "AGACCOUNTS" or any derivation. o Birthdays and other personal information such as addresses and phone numbers. o Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc. o Any of the above spelled backwards. o Any of the above preceded or followed by a digit (e.g., secret1, 1secret) Strong passwords have the following characteristics: · Contain both upper and lower case characters (e.g., a-z, A-Z) · Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./) · Are at least eight alphanumeric characters long. · Are not a word in any language, slang, dialect, jargon, etc. · Are not based on personal information, names of family, etc. · Passwords should never be written down or stored on-line. Try to create passwords that can be easily

remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. B. Password Protection Standards Do not use the same password for IAAD accounts as for other non-IAAD access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various IAAD access needs. Also, select a separate password to be used for a Windows account and a UNIX account. Do not share IAAD passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential IAAD information. Here is a list of "dont's": · Don't reveal a password over the phone to ANYONE · Don't reveal a password in an email message · Don't reveal a password to the boss · Don't talk about a password in front of others · Don't hint at the format of a password (e.g., "my family name") · Don't reveal a password on questionnaires or security forms · Don't share a password with family members · Don't reveal a password to co-workers while on vacation If someone demands a password, refer them to this document or have them speak to the Information Security Manager of your office. Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Internet Explorer, Messenger). Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption. Change passwords at least once every six months (except system-level/ corporate e-mail account passwords which must be changed quarterly). The recommended change interval is every four months. If an account or password is suspected to have been compromised, report the incident to the Information Security Manager / System Administrator and change all passwords. Password cracking or guessing may be performed on a periodic or random basis by Information Security Officer or his delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it. C. Application Development Standards Application developers must ensure their programs contain the following security precautions. Applications: · should support authentication of individual users, not groups. · should not store passwords in clear text or in any easily reversible form. · should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password. · should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible. D. Use of Passwords and Passphrases for Remote Access Users Access to the IAAD Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase. E. Passphrases Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access. Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: "The*?#>*@TrafficOnTheRingRoadWas*&#!#ThisMorning" All of the rules above that apply to passwords apply to passphrases. 5.0 Enforcement Any employee found to have violated this policy may be subject to disciplinary action. 6.0 Definitions Terms Definitions Application Administration Account Any account that is for the administration of an application (e.g., Oracle database administrator, VLC Admin account).

4. Anti-Virus Policy 1.0 Overview Computers infected with viruses or malicious code could jeopardize information security by contaminating data. This policy provides controls to protect against such attacks. Computer viruses are data destructive programs written with the intent of copying and spreading the destruction to other computers and programs. A typical virus is a small computer program that, as part of its operations, reproduces itself by making copies of itself and inserting these copies into uninfected programs or data files. This insertion process takes only a fraction of a second, a virtually undetectable delay. The infected program will subsequently execute the virus code during its normal processing. In addition to its ability to reproduce, the virus may cause damage to the programs, data, or equipment, or it may perform some other function that is relatively harmless. 1.1 Computer virus types Viruses are classified depending on how they infect the computer systems on a network and they are of the following types. Boot Viruses They attack the boot record, the master boot record, the File Allocation Table (FAT), and the partition table of a computer hard drive. They generally propagate from an infected diskette placed in the disk drive of a computer while it starts or otherwise. Joshi and Michelangelo are examples of boot sector viruses. File Viruses (Trojan Horse) Trojan horse, also called RAT (remote access Trojan, or remote access trapdoor) are examples of file virus. They attack program files (e.g. .exe; .com; .sys, .drv; .ovl; .bin; .scr etc.) by attaching themselves to executable files. The virus waits in memory for users to run another program and use the event to infect and replicate. Macro virus These virus attack programs that runs macros. Most common are in Microsoft word documents. These virus starts when a document or a template file in which it is embedded is opened by an application. Example: Melissa. Stealth Viruses These disguise their actions and can be passive or active. Passive viruses can increase the file size yet present the size of the original thus preventing detection, while active ones attack the anti virus software rendering them useless. Example: Tequila. Multipartite Viruses These have characteristics of both the boot and program viruses. Example: Natas Encrypted virus These have built in encryption software code that masks the viral code making it difficult to identify and detect the virus. Example: Cascade Polymorphic Viruses These are growing rapidly and have an inbuilt mechanism that changes the virus signature. Example: SMEG Worms A worm is an independent program that reproduces by copying itself from one system to another usually over a network. They infiltrate legitimate programs and alter or destroy data. Unlike other virus worms cannot replicate itself. Logic Bombs Logic Bombs are programs that are triggered by a timing device such as a date or an event and are highly destructive. 2.0 Purpose To establish requirements which must be met by all stand-alone computers, and computers connected to IAAD's networks to ensure effective virus detection and prevention. 3.0 Scope This policy applies to all IAAD computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file /ftp /proxy servers. 4.0 Policy All IAAD PC-based computers must have IAAD's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. It is the responsibility of the primary user of the PC to ensure that that anti-virus software is updated regularly. Virus-infected computers must be removed from the network until they are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into IAAD's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy. Noted exceptions: Machines with operating systems other than those based on Microsoft products are excepted at the current time. 5.0 Anti-virus Guidelines and Best Practices · Always run the standard, supported anti-virus software provided by the Head Office. Download and install anti-virus software updates as they become available. The antivirus updates may be picked up from over the internet from the Anti-

virus vendor’s sites, where computers have access to the Internet. Each IAAD office should however configure a management console to update the antivirus software of all the PCs on the network, after downloading the update centrally from the internet. If all computers are not on the Local Area Network, it is the responsibility of the EDP Cell of the office to make weekly Anti-virus updates made available to all PC users in some removable media (CD, Floppy). · For standalone PC’s the antivirus software loaded into PC should be automatically enabled for checking viruses. · Application based Antivirus should be installed for applications like MS-Exchange, Lotus Notes etc. · NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash. · Delete spam, chain, and other junk email without forwarding, in keeping with IAAD's Acceptable Use Policy. · Never download files from unknown or suspicious sources. · Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so. · Always scan a floppy diskette/USB Memory stick-Thumb drive from an unknown source for viruses before using it. · Back-up critical data and system configurations on a regular basis and store the data in a safe place. · External media (ex. Floppy, CD’s) is one of the most potent medium for transmission of viruses’, hence it must not be used in the network except for a few pre determined management PC’s. · Network based critical applications like GPF and VLC should be isolated. No computer on the PC should have access to the internet, or have removable storage devices like Floppy disks/ CD-ROMS, USB ports activated. Only few Management consoles may have access to such removable devices, and these PCs should be protected with Antivirus software with due care being taken in transferring files to the network. · Follow the prescribed password policy. Complex password makes it difficult to crack password files on compromised systems/computers. This helps to prevent damage when a computer is compromised. · Apply the latest patches for web browsers or else simply visiting a compromised web site can cause infection. 6.0 Enforcement Any employee found to have violated this policy may be subject to disciplinary action.

Part-IV

Guidelines and Methodologies

1. IT Security Training Introduction: Organizations cannot protect the integrity, confidentiality, and availability of information in today’s highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them. Everyone, therefore, needs basic training in IT security concepts and procedures. Noting the vast scope of IT Security, and the needs of employees of our department functioning at various levels with different job responsibility, the training may be organized at three distinct levels of IT security training: Beginning, Intermediate, and Advanced. 1. Level-1: Beginning: Security Basics 1.1 Approach: Level 1 Training will focus on IT Security Literacy. IT Security literacy refers to an individual’s familiarity with—and ability to apply—a core knowledge set (i.e., “IT security basics”) needed to protect electronic information and systems. All individuals who use computer technology or its output products, regardless of their specific job responsibilities, must know IT security basics and be able to apply them. 1.2 Course Outline: The core set of IT security terms and concepts is presented as the “ABC’s of Information Technology Security,” 26 items related to the alphabet, as summarized in the box below, and described briefly

in Annexure-IV-1-1. This memory tool approach aids the learning process while communicating fundamental IT security concepts. The course material developed under this model will build on the memory tool approach to learning. Besides, the employee responsibility vis-à-vis IT Security needs to be explained to the participants. ABC's OF INFORMATION TECHNOLOGY SECURITY A Assets - Something of value requiring protection (hardware, software, data, reputation) B Backup - The three most important safeguards - backup, backup, backup C Countermeasures and Controls - Prevent, detect, and recover from security incidents D Data Accredition Authority and Other Officials - Manage and accept risk and authorize the system to operate E Ethics - The body of rules that governs an individual's behaviour. F Firewalls and Separation of Duties - Minimize the potential for "incident encroachment" G Goals - Confidentiality, Integrity, and Availability (CIA) H Hackers/Crackers - Intruders who are threats to any system I Individual Accountability/Responsibility - Individuals responsible for their own actions J Job Description/Job Function - Defines the individual's roles within the organization K Keys to Incident Prevention - Awareness, compliance, common sense L Laws and Regulations - Establish basic control/security objectives M Model Framework - Relates training needs to roles and responsibilities N Need to Know - Limits access to data, sets objective for ongoing learning O Ownership - Establishes responsibility/accountability for asset protection P Policies and Procedures - What to accomplish and how to accomplish it Q Quality Assurance/Quality Control - Ensure the integrity of the process R Risk Management - Balances potential adverse impact against safeguard cost S Security Training - The best return on investment of any security safeguard T Threats - Are always present, and generally occur when least expected U Unique Identifiers - Provide for individual accountability and facilitate access control V Vulnerabilities - Security weaknesses through which threats impact the system W Waste, Fraud, and Abuse - The three primary impacts of a security incident X eXpect the uneXpected - Don't assume that because something hasn't happened, it won't Y You - Your actions/inactions are critical to maintaining an effective security environment Z Zoning/Compartmentalization - Establish security layers and minimize incident impact

1.3 Duration: The training may be of two days duration. This course may be conducted by all training institutes, RTIs, RTCs and iCISA for officers and staff of different levels.

2 Level-2: Intermediate (Literacy) 2.1 Approach The literacy level is the first solid step of the IT security training level, where the knowledge obtained through training can be directly related to the individual's role in his or her specific organization. Although the curriculum framework, presented below, provides a generic outline for material to be included in literacy training throughout government, it is imperative that the instructor relate the actual course content to the organization's unique culture and mission requirements. At the literacy level, the material should be presented as an introduction of the concepts and topics only. 2.2 Course Outline: The course would focus on the following topics: o IT Security Policy of IAAD, and its direct relation to Organisation's IT assets. o An Introduction to Risk Management, and understanding of various threats and vulnerabilities relevant to the Department's IT Assets. o Exposure to selected Management, Acquisition / Development/ Installation / Implementation, Operational and Technical Controls. The detailed course outline is given in Appendix IV-1-2 2.3 Duration: The training may be of 4 days duration. This training may be conducted by all training institutes, RTIs, RTCs and iCISA for officers and staff of different levels. Preferably, this may be targeted at officers above the rank of Section Officer. [C1]Suggest discouraged to use.

3. Level-3: Advanced

3.1 Approach This course builds on the skills imparted through the intermediate level security training. The objective here is to equip the trainees with strong theoretical grounding in IT Security Concepts, such that they are able to apply the same in their day to day functioning. This training is primarily meant for IAAS Officers, and officers above the rank of Accounts officers who are directly working in EDP environment.

3.2 Course Outline: The course would focus on the following topics:

o Detailed coverage of the IT Security Policy of IAAD, including all Security Domains, IT Act 2000

o Risk Management Framework, and understanding of various threats and vulnerabilities relevant to our IT Assets.

o System Interconnection and Information Sharing

o Management, Acquisition / Development/ Installation / Implementation, Operational and Technical Controls.

The detailed course outline is given in Appendix-IV-1-3

3.3 Duration:

The Advanced Level IT Security training may be of 6 days duration. This course may be conducted by iCISA (International Centre for Information Systems and Audit), NOIDA, and NAAA, Shimla (National Academy of Audit and Accounts).

Appendix-IV-1-1 (Basic Level)

IT Security ABC's - Terms and Concepts

Assets - Assets are something of value that requires protection. The value of an asset may be monetary or non-monetary. For example, a computer system clearly has a monetary value that may be expressed in terms of its cost of acquisition or replacement. Data, however, is an asset that may have a monetary value (the cost to acquire), a non-monetary value (loss of public confidence regarding data accuracy), or both.

Backup - Backup for data and/or processes are critical safeguards in any IT security

environment. The concept of backup includes creation and testing of disaster recovery and continuity of operations plans as well as preparation of copies of data files that are stored "out of harm's way."

Countermeasures and Controls - Countermeasures, controls, and safeguards are terms that are often used synonymously. They refer to the procedures and techniques used to prevent the occurrence of a security incident, detect when an incident is occurring or has occurred, and provide the capability to respond to or recover from a security incident. A safeguard may be a password for a user identifier, a backup plan that provides for offsite storage of copies of critical files, audit trails that allow association of specific actions to individuals, or any of a number of other technical or procedural techniques. Basically, a safeguard is intended to protect the assets and availability of IT systems.

DAA and Other Officials - Individuals are responsible for allocating resources. Resources may be allocated to address IT security issues or any of a number of other competing organizational needs. The individual who has such authority for a specific IT system may be termed a Designated Accrediting Authority (DAA), Approving Authority, Authorizing Official, Recommending Official, or other titles specific to an organization. Whatever the title, the individual who has the authority to allocate resources is also responsible for balancing risks and costs and accepting any residual risks in making those decisions. The accrediting authorities are often helped in these decisions by certifying authorities who provide assessments of the technical adequacy of the current security environment and recommendations for resolving deficiencies or weaknesses.

Ethics - the body of rules that governs an individual's behaviour. It is a product of that individual's life experiences and forms a basis for deciding what is right and wrong when making decisions. In today's environment, ethics are, unfortunately, situational (i.e., an individual's definition of what is right and wrong changes depending on the nature of a particular situation). For example, an individual may believe that it is wrong to break into someone's house, but does not think that it is wrong to break into someone's computer system.

Firewalls and Separation of Duties - Firewalls and separation of duties have similar structures and complementary objectives: a firewall is a technical safeguard that provides separation between activities, systems, or system components so that a security failure or weakness in one is contained and has no impact on other activities or systems (e.g., enforcing separation of the Internet from a Local Area Network). Separation of duties similarly provides separation, but its objective is to ensure that no single individual (acting alone) can compromise an application. In both cases, procedural and technical safeguards are used to enforce a basic security policy that high risk activities should be segregated from low risk activities and that one person should not be able to compromise a system.

Goals - The goals of an IT security program can be summarized in three words: *confidentiality* - data must be protected against unauthorized disclosure; *integrity* - IT systems must not permit processes or data to be changed without authorization; and *availability* -authorized access to IT systems must be assured.

Hackers/Crackers - The term "hacker" was originally coined to apply to individuals who focused on learning all they could about IT, often to the exclusion of many other facets of life (including sleeping and eating). A "cracker" is any individual who uses advanced knowledge of networks or the Internet to compromise network security. Typically, when the traditional hacker compromised the security of an IT system, the objective was academic (i.e., a learning exercise), and any resulting damage or destruction was unintentional. Currently, the term hacker is being more widely used to describe any individual who attempts to compromise the security of an IT system, especially those whose intention is to cause disruption or obtain unauthorized access to data. Hacker/cracker activity generally gets high press coverage even though more mundane security incidents caused by unintentional actions of authorized users tend to cause greater disruption and loss.

Individual Accountability/Responsibility - A basic tenet of IT security is that individuals must be accountable for their actions. If this is not followed and enforced, it is not possible to successfully prosecute those who intentionally damage or disrupt systems, or to train those whose actions have unintended adverse effects. The concept of individual accountability drives the need for many security safeguards such as user identifiers, audit trails, and access authorization rules.

Job Description/Job Function - To provide individuals with the training necessary to do their job, and to establish appropriate safeguards to enforce individual accountability, it is necessary to know what functions an individual is authorized to perform (i.e., their role(s) within the organization). Some times this is accomplished using formalized/written job descriptions. In other situations, such assessments are based on analysis of the functions performed.

Keys to Incident Prevention - Many IT security incidents are preventable if individuals incorporate three basic concepts into their day-to-day activities: one, awareness - individuals should be aware of the value of the assets they use to do their job and the nature of associated threats and vulnerabilities; two, compliance - individuals should comply with established safeguards (e.g., scanning diskettes, changing passwords, performing backups); and three, common sense - if something appears too good to be true, it generally is.

Laws and Regulations - The Government of India has passed the IT Act 2000. These laws have been augmented with regulations and guidance regarding their applicability to IT systems. Private industry generally grounds its security policies on the impact on profitability and potential risk of lawsuits, as there are few specific legal requirements.

Model Framework - This document presents a model framework for IT security training. The model framework describes individual training needs relative to job function or role within the organization. The model recognizes that an individual's need for IT security training will change, both in scope and depth, relative to their organizational responsibilities.

Need to Know - Need to Know is addressed from two perspectives: first, a need for access to information to do a job; and second, need to know as a driver for continued learning. In the first case, access to information and processes should be restricted to that which the individual requires to do their job. This approach minimizes the potential for unauthorized activities, and maximizes the potential that the individual knows and understands the nature of the threats and vulnerabilities associated with their use or maintenance of an IT system; and second, given the rate of technological change, individuals need to know the characteristics of those technologies so they may be better able to address specific vulnerabilities.

Ownership - Responsibility for the security of an IT system or asset must be assigned to a single, identifiable entity, and to a single, senior official within that entity. This provides for accountability for security failures and establishment of the chain of command that authorizes access to and use of system assets. This concept of individual responsibility and authority is generally termed ownership or stewardship. The ownership of an asset (particularly data) is generally retained, even when that asset is transferred to another organization. For example, tax data shared with other Federal and state agencies by the Internal Revenue Service must be secured in accordance with the Internal Revenue Code.

Policies and Procedures - IT security safeguards are intended to achieve specific control objectives. These objectives are contained within security policies that should be tailored to the needs of each IT system. Procedures define the technical and procedural safeguards that have been implemented to enforce the specified policies. IT security procedures may be documented in a security plan.

Quality Assurance/Quality Control - Quality Assurance and Quality Control are two processes that are used to ensure the consistency and integrity of security safeguards. Specifically, these processes are intended to ensure that security countermeasures perform as specified, under all workload and operating conditions.

Risk Management - Risk management is the process whereby the threats, vulnerabilities, and potential impacts from security incidents are evaluated against the cost of safeguard implementation. The objective of Risk Management is to ensure that all IT assets are afforded reasonable protection against waste, fraud, abuse, and disruption of operations. Risk Management is growing in importance as the scope of potential threats is growing while available resources are declining.

Security Training - Security training is the sum of the processes used to impart the body of knowledge associated with IT security to those who use, maintain, develop, or manage IT systems. A well trained staff can often compensate for weak technical and procedural safeguards. Security training has been demonstrated to have the greatest return on investment of any technical or procedural IT security safeguard.

Threats - Threats are actions or events (intentional or unintentional) which, if realized, will result in waste, fraud, abuse, or disruption of operations. Threats are always present, and the rate of threat occurrence can not be controlled. IT security safeguards, therefore, must be designed to prevent or minimize any impact on the affected IT system.

Unique Identifiers - A unique identifier is a code or set of codes that provide a positive association between authorities and actions to individuals. Safeguards must be in place to ensure that an identifier is used only by the individual to whom it is assigned.

Vulnerabilities - Vulnerabilities are weaknesses in an IT system's security environment. Threats may exploit or act through a vulnerability to adversely affect the IT system. Safeguards are used to mitigate or eliminate vulnerabilities.

Waste, Fraud, and Abuse - Waste, fraud, and abuse are potential adverse impacts that may result from a breakdown in IT security. Waste, fraud, and abuse are specifically identified as potential impacts in government-wide policy.

eXpect the uneXpected - IT security safeguards target unauthorized actions. Unauthorized actions (acts by individuals or Acts-of-God) can take many forms and can occur at any time. Thus, security safeguards should be sufficiently flexible to identify and respond to any activity that deviates from a pre-defined set of acceptable actions.

You - You are responsible and will be held accountable for your actions relative to an IT system or its associated data. You can strengthen or weaken an IT security environment by your actions or inactions. For example, you can strengthen an IT environment by changing passwords at appropriate intervals and weaken it by failing to do so.

Zoning/Compartmenting - Zoning/Compartmenting is a concept whereby an application is segmented into independent security environments. A breach of security would require a security failure in two or more zones/compartments before the application is compromised. This layered approach to security can be applied within physical or technical environments associated with an IT system.

Appendix-IV-1-2(Intermediate Level)

Intermediate Level Security Training Course Outline

1. IT Security Policy of IAAD

a. IT Security Policy

b. Brief Introduction to the various Security Domains

c. Explanation of the core Policies.

2. Laws and Regulations:

a. Overview of the IT Security Policy of IAAD

b. IT Act 2000(Relevant Clauses)

c. Organization specific policies and procedures

d. Tangible and intangible IT resources (assets)

e. Laws concerning copyrighted software

3. The Organization and IT Security

a. Organization mission(s)

b. How information technology supports the mission(s)

c. Reliance on IT systems for mission accomplishment

d. Changing IT security issues and requirements

4. Sensitivity

a. Categorization of system sensitivity

i. Criticality

ii. Unauthorized use

iii. Reliability

b. Categorization of information sensitivity

c. Sensitive information in general

d. Need to know

e. Authorized access

f. Unauthorized disclosure

g. IT asset protection requirements

h. The organization’s need for confidentiality of its information, Adverse consequences of unauthorized information disclosure

i. The organization’s need for integrity of its information

j. Corruption of information (Accidental, Intentional)

k. Adverse consequences if public or other users do not trust integrity and reliability of information

l. The organization’s need for availability of its information and IT systems

m. Adverse consequences of system or information unavailability

n. Public dependence on information

o. Internal or external user’s dependence on information

5. Risk Management

a. Managing risk (Threats, Vulnerabilities, Risk)

b. Relationships between threats, vulnerabilities, risks

c. Threats from “authorized system users”

d. Malicious software programs and virus threats

e. Examples of security controls for:

i. Confidentiality protection

ii. Availability protection

iii. Integrity protection

f. Contingency-disaster recovery planning: Importance of plan to deal with unexpected problems, Importance of testing plan and applying lessons learned

6. Management Controls

a. System/application-specific policies and procedures

b. Standard operating procedures

c. Personnel security

i. Roles and responsibilities

ii. Separation of duties

iii. Role-based access controls

7. Acquisition/Development/Installation/Implementation Controls

a. System life cycle stages and functions

b. IT security requirements in system life cycle stages

8. Operational Controls

a. Physical and environmental protection

i. Physical access controls

ii. Intrusion detection

iii. Fire/water/moisture/heat/electrical maintenance

b. Contingency planning

i. Importance of developing and testing contingency/disaster recovery plans

ii. Importance of users providing accurate information about processing needs, allowable down time and applications that can wait

iii. Responsibility for backup copies of data files and software programs

iv. Simple user contingency planning steps

9. Technical Controls

a. How technical (role-based access) controls support management (security rules) controls

i. User identification and passwords/tokens

ii. User role-based access privileges

iii. Public access controls

b. User actions to prevent damage from malicious software or computer virus attacks

i. Organization specific procedures for reporting virus incidents

ii. Technical support and help from security incident response teams

iii. Software products to scan, detect and remove computer viruses

Appendix-IV-1-3(Advanced Level)

Advanced Level Security Training Course Outline

1. IT Security Policy of IAAD

a. IT Security Policy

b. Explanation of the various Security Domains

c. Explanation of the core Policies.

2. Laws and Regulations:

a. Brief Overview of the IT Security Policy of IAAD

b. IT Act 2000(Relevant Clauses)

c. Organization specific policies and procedures

d. Tangible and intangible IT resources (assets)

e. Current and emerging social issues that can affect IT assets

f. Laws concerning copyrighted software

3. The Organization and IT Security

a. Organization mission(s)

b. How information technology supports the mission(s)

c. Reliance on IT systems for mission accomplishment

d. Changing IT security issues and requirements

4. System Interconnection and Information Sharing

a. Increased vulnerabilities of interconnected systems and shared data

b. Responsibilities of system or information owner organizations if systems have external users or clients

c. Responsibility of users or clients for notifying system owners of security requirements

d. Sharing information on system controls with internal and external users and clients

e. Electronic mail security concerns

f. Electronic commerce

g. Electronic Fund Transfer

h. Electronic Data Interchange

i. Digital/electronic signatures

j. Monitoring user activities

5. Sensitivity

a. Categorization of system sensitivity

i. Criticality

ii. Unauthorized use

iii. Reliability

b. Categorization of information sensitivity

c. Sensitive information in general

d. Need to know

e. Authorized access

f. Unauthorized disclosure

g. IT asset protection requirements

h. The organization's need for confidentiality of its information, Adverse consequences of unauthorized information disclosure

i. The organization’s need for integrity of its information

j. Corruption of information (Accidental, Intentional)

k. Adverse consequences if public or other users do not trust integrity and reliability of information

l. The organization’s need for availability of its information and IT systems

m. Adverse consequences of system or information unavailability

n. Public dependence on information

o. Internal or external user’s dependence on information

6. Risk Management

a. Managing risk (Threats, Vulnerabilities, Risk)

b. Relationships between threats, vulnerabilities, risks

c. Threats from “authorized system users”

d. Increased threats and vulnerabilities from connection to external systems and networks

e. “Hacker” threats

f. Malicious software programs and virus threats

g. Types of security controls (safeguards, countermeasures): Management controls, Acquisition/development/installation/implementation controls, Operational controls, Security awareness and training controls, Technical controls

h. How different categories of controls work together

i. Examples of security controls for:

i. Confidentiality protection

ii. Availability protection

iii. Integrity protection

j. Added security controls for connecting external systems and networks

k. Protecting assets through IT security awareness and training programs

l. Contingency-disaster recovery planning: Importance of plan to deal with unexpected problems, Importance of testing plan and applying lessons learned

m. “Acceptable levels of risk” vs. “absolute protection from risk”

n. “Adequate” and “appropriate” controls

i. Unique protection requirements of IT systems and information

ii. Severity, probability, and extent of potential harm

iii. Cost effective/cost benefits

iv. Reduction of risk vs. elimination of risk

o. Working together with other security disciplines

p. Importance of internal and external audits, reviews, and evaluations in security decisions

7. Management Controls

a. System/application-specific policies and procedures

b. Standard operating procedures

c. Personnel security

i. Roles and responsibilities

ii. Separation of duties

iii. Role-based access controls

d. System rules of behaviour contribute to an effective security environment

i. Organization-specific user rules

ii. System-specific user rules

- Assignment and limitation of system privileges
- Intellectual property/Copyright issues
- Remote access and work at home issues
- Official vs. unofficial system use
- Individual accountability
- Sanctions or penalties for violations

e. Individual accountability contributes to system and information quality

f. IT security awareness and training

8. Acquisition/Development/Installation/Implementation Controls

a. System life cycle stages and functions

b. IT security requirements in system life cycle stages

c. Formal system security plan for management of a system

d. Definition of system protection needs

e. Identification of responsible people

f. Identification of system security controls in-place or planned and milestone dates for implementation of planned controls

g. Relationship of configuration and change management programs to IT security goals

h. Testing system security controls and certification

i. Senior manager approval (accredit) an IT system for operation

9. Operational Controls

a. Physical and environmental protection

i. Physical access controls

ii. Intrusion detection

iii. Fire/water/moisture/heat/electrical maintenance

iv. Mobile and portable systems

b. Contingency planning

i. Importance of developing and testing contingency/disaster recovery plans

ii. Importance of users providing accurate information about processing needs, allowable down time and applications that can wait

iii. Responsibility for backup copies of data files and software programs

iv. Simple user contingency planning steps

10. Technical Controls

a. How technical (role-based access) controls support management (security rules) controls

i. User identification and passwords/tokens

ii. User role-based access privileges

iii. Public access controls

b. How system controls can allow positive association of actions to individuals

i. Audit trails

ii. System monitoring

c. Recognizing attacks by hackers, authorized or unauthorized users

i. Effects of hacker attack on authorized users

ii. Unauthorized use or actions by authorized users

iii. Reporting incidents

d. User actions to prevent damage from malicious software or computer virus attacks

i. Organization specific procedures for reporting virus incidents

ii. Technical support and help from security incident response teams

iii. Software products to scan, detect and remove computer viruses

e. Role of cryptography in protecting information

2. Risk Assessment Methodology

1. Introduction:

An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the *organization and its ability to perform their mission*, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help the Department to better manage IT-related mission risks.

1.1 Objective

The objective of performing risk management is to enable the organization to accomplish its mission(s) (1) by better securing the IT systems that store, process, or transmit organizational information; (2) by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and (3) by assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management.

2. Risk Management Overview

2.1 Importance of risk management Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. Section 3 of this document describes the risk assessment process, which includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. Section 4 describes risk mitigation, which refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. Section 5 discusses the continual evaluation process and keys for implementing a successful risk management program. The system authorizing official is responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk before authorizing (or accrediting) the IT system for operation.

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations missions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

2.2 Integration of Risk Management into SDLC

Effective risk management must be totally integrated into the SDLC. An IT system's SDLC has five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. In some cases, an IT system may occupy several of these phases at the same time. However, the risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC. Table 2-1 describes the characteristics of each SDLC phase and indicates how risk management can be performed in support of each phase.

Table 2-1 Integration of Risk Management into the SDLC

SDLC Phases	**Phase Characteristics**	**Support from Risk Management Activities**
Phase 1.Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented	Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations (strategy)
Phase 2.Development or Acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design trade-offs during system development
Phase 3.Implementation	The system security features should be configured, enabled, tested, and verified	The risk management process supports the assessment of the system implementation against its requirements and within its modelled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4.Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	Risk management activities are performed for periodic system reauthorization (or re-accreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)

Phase 5.Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner

2.3 Key Roles

Risk management is a management responsibility. This section describes the key roles of the personnel who should support and participate in the risk management process.

Senior Management

Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management.

System and Information Owners

The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. Typically the system and information owners are responsible for changes to their IT systems. Thus, they usually have to approve and sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware). The system and information owners must therefore understand their role in the risk management process and fully support this process.

Business and Functional Managers

The managers responsible for business operations and IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment. Their involvement in the risk management process enables the achievement of proper security for the IT systems.

IT Security Practitioners

IT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts; security consultants) are responsible for proper implementation of security requirements in their IT systems. As changes occur in the existing IT system environment, the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems.

Security Awareness Trainers (Security/Subject Matter Professionals).

To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training. Therefore, the IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.

3. Risk Assessment

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, as discussed in Section 4. *Risk* is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization. To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data). The risk assessment methodology encompasses nine primary steps, which are described in Sections 3.1 through 3.9

- Step 1-System Characterization (Section 3.1)
- Step 2-Threat Identification (Section 3.2)
- Step 3-Vulnerability Identification (Section 3.3)
- Step 4-Control Analysis (Section 3.4)
- Step 5-Likelihood Determination (Section 3.5)

- Step 6-Impact Analysis (Section 3.6)

- Step 7-Risk Determination (Section 3.7)

- Step 8-Control Recommendations (Section 3.8)

- Step 9-Results Documentation (Section 3.9).

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed.

3.1 Step 1: System Characterization

In assessing risks for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk.

The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows:

- Hardware

- Software

- System interfaces (e.g., internal and external connectivity)

- Data and information

- Persons who support and use the IT system

- System mission (e.g., the processes performed by the IT system)

- System and data criticality (e.g., the system’s value or importance to an organization)

- System and data sensitivity.

For a system that is in the initiation or design phase, system information can be derived from the design or requirements document. For an IT system under development, it is necessary to define key security rules and attributes planned for the future IT system. System design documents and the system security plan can provide useful information about the security of an IT system that is in development. For an operational IT system, data is collected about the IT system in its production environment, including data on system configuration, connectivity, and documented and undocumented procedures and practices. Therefore, the system description can be based on the security provided by the underlying infrastructure or on future security plans for the IT system.

Information-Gathering Techniques

Any, or a combination, of the following techniques can be used in gathering information relevant to the IT system within its operational boundary:

- Questionnaire.

- On-site Interviews.

- Document Review.

- Use of Automated Scanning Tool.

Information gathering can be conducted throughout the risk assessment process, from Step 1 (System Characterization) through Step 9 (Results Documentation).

Output from Step 1:

Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundary

3.2 Step 2: Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat (Section 3.5), one must consider threat-sources, potential vulnerabilities (Section 3.3), and existing controls (Section 3.4).

Threat-Source Identification:

A threat-source is defined as any circumstance or event with the potential to cause harm to an IT system. The common threat-sources can be natural, human, or environmental.

Motivation and Threat Actions:

Motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources.

Output from Step 2: A threat statement containing a list of threat-sources that could exploit system vulnerabilities

3.3 Step 3: Vulnerability Identification

The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

(*Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy*)

3.3.1 Vulnerability Sources

The technical and non-technical vulnerabilities associated with an IT system's processing environment can be identified via the information-gathering techniques described in Section 3.1

Documented vulnerability sources that should be considered in a thorough vulnerability analysis include, but are not limited to, the following:

- Previous risk assessment documentation of the IT system assessed

- The IT system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports

- System software security analyses.

3.3.2 System Security Testing

Proactive methods, employing system testing, can be used to identify system vulnerabilities efficiently, depending on the criticality of the IT system and available resources (e.g., allocated funds, available technology, persons with the expertise to conduct the test).

Test methods include

- Automated vulnerability scanning tool
- Security test and evaluation (ST&E)
- Penetration testing.

3.3.3 Development of Security Requirements Checklist

During this step, the risk assessment personnel determine whether the security requirements stipulated for the IT system and collected during system characterization are being met by existing or planned security controls. Typically, the system security requirements can be presented in table form, with each requirement accompanied by an explanation of how the system's design or implementation does or does not satisfy that security control requirement.

A security requirements checklist contains the basic security standards that can be used to systematically evaluate and identify the vulnerabilities of the assets (personnel, hardware, software, and information), non-automated procedures, processes, and information transfers associated with a given IT system in the following security areas:

- Management
- Operational
- Technical.

The results of the checklist (or questionnaire) can be used as input for an evaluation of compliance and non-compliance. This process identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

Output from Step 3

: A list of the system vulnerabilities that could be exercised by the potential threat-sources

3.4 Step 4: Control Analysis

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment (Step 5 below), the implementation of current or planned controls must be considered. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

Development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner.

Output from Step 4

: List of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event

3.5 Step 5: Likelihood Determination

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- *Threat-source motivation and capability*

- *Nature of the vulnerability*

- *Existence and effectiveness of current controls.*

The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low.

Output from Step 5: Likelihood rating (High, Medium, Low)

3.6 Step 6: Impact Analysis

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability.

Before beginning the impact analysis, it is necessary to obtain the following necessary information as discussed in Section 3.1:

- *System mission (e.g., the processes performed by the IT system)*

- *System and data criticality (e.g., the system's value or importance to an organization)*

- *System and data sensitivity.*

This information would be more easily available if a Business impact analysis, and Asset criticality assessment has been done for the organisation. Business impact analysis [BIA] prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality.

Regardless of the method used to determine how sensitive an IT system and its data are, the system and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s).

Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

- *Loss of Integrity. System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts.*

- *Loss of Availability. If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected.*

- *Loss of Confidentiality. System and data confidentiality refers to the protection of information from unauthorized disclosure. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.*

Quantitative versus Qualitative Assessment

In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments.

While there are advantages and disadvantages in both approaches, we may adopt a qualitative assessment as it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.

The impact assessment may be made as:

- *High: Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.*

- *Medium: Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.*

- *Low: Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.*

Output from Step 6: Magnitude of impact (High, Medium, or Low)

3.7 Step 7: Risk Determination

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of

- *The likelihood of a given threat-source's attempting to exercise a given vulnerability*

- *The magnitude of the impact should a threat-source successfully exercise the vulnerability*

- *The adequacy of planned or existing security controls for reducing or eliminating risk.*

To measure risk, a risk scale and a risk-level matrix must be developed.

3.7.1 Risk-Level Matrix

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. Table 2-2 below shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact categories. The matrix below is a 3 x 3 matrix of threat likelihood (High, Medium, and Low) and threat impact (High, Medium, and Low).

Table 2-2: Risk-Level Matrix

Impact Threat Likelihood	Impact		
	Low(10)	Medium(50)	High(100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

3.7.2 Description of Risk Level

Based on the above matrix, the risk level can be identified as High, Medium or Low, which in turn is a function of the likelihood and Impact.

This risk scale, with its ratings of High, Medium, and Low, represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

- ➢ High: If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.

- ➢ Medium: If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.

- ➢ Low: If an observation is described as low risk, the system’s DAA must determine whether corrective actions are still required or decide to accept the risk.

Output from Step 7:

Risk level (High, Medium, Low)

3.8 Step 8: Control Recommendations

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level.

It should be noted that not all possible recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, should be conducted for the proposed recommended controls. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.

Output from Step 8:

Recommendation of control(s) and alternative solutions to mitigate risk

3.9 Step 9: Results Documentation

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing. A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses.

Output from Step 9:

Risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation

4. Risk Mitigation

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

4.1 Risk Mitigation Options

Risk mitigation is a systematic methodology used by senior management to reduce mission risk. Risk mitigation can be achieved through any of the following risk mitigation options:

- *Risk Assumption: To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level*

- *Risk Avoidance: To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)*

- *Risk Limitation: To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)*

- *Risk Planning: To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls*

- *Research and Acknowledgment: To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability*

- *Risk Transference: To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.*

The goals and mission of an organization should be considered in selecting any of these risk mitigation options. It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm.

4.2 Risk Mitigation Strategy:

The following rules of thumb, provides guidance on actions to mitigate risks from intentional human threats:

i. *When vulnerability (or flaw, weakness) exists: Implement assurance techniques to reduce the likelihood of a vulnerability's being exercised.*

ii. *When a vulnerability can be exercised: Apply layered protections, architectural designs, and administrative controls to minimize the risk of or prevent this occurrence.*

iii. When the attacker's cost is less than the potential gain: Apply protections to decrease an attacker's motivation by increasing the attacker's cost (e.g., use of system controls such as limiting what a system user can access and do can significantly reduce an attacker's gain).

iv. When loss is too great: Apply design principles, architectural designs, and technical and non-technical protections to limit the extent of the attack, thereby reducing the potential for loss.

The strategy outlined above, with the exception of the third list item (When the attacker's cost is less than the potential gain), also applies to the mitigation of risks arising from environmental or unintentional human threats (e.g., system or user errors). (Because there is no attacker, no motivation or gain is involved.)

4.3 Approach For Control Implementation:

When control actions must be taken, the following rule applies: Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities.

The following risk steps may be followed:

- *Step 1 Prioritize Actions: Based on the risk levels presented in the risk assessment report, the implementation actions are prioritized.*

- *Step 2 Evaluate Recommended Control Options: The objective is to select the most appropriate control option for minimizing risk.*

- *Step 3 Conduct Cost-Benefit Analysis*

- *Step 4 Select Control: On the basis of the results of the cost-benefit analysis, management determines the most cost-effective control(s) for reducing risk to the organization's mission.*

- *Step 5 Assign Responsibility: To personnel (in-house, external agency) who have the appropriate expertise and skill-sets to implement the selected control.*

- *Step 6 Develop a Safeguard Implementation Plan: The safeguard implementation plan prioritizes the implementation actions and projects the start and target completion dates.*

- *Step 7 Implement Selected Control(s): Depending on individual situations, the implemented controls may lower the risk level but not eliminate the risk, leaving behind, residual risk.*

4.4 Control Categories :

In implementing recommended controls to mitigate risk, an organization should consider technical, management, and operational security controls, or a combination of such controls, to maximize the effectiveness of controls for their IT systems and organization.

4.4.1 Technical Security Controls:

These controls may range from simple to complex measures and usually involve system architectures; engineering disciplines; and security packages with a mix of hardware, software, and firmware.

Technical controls can be grouped into the following major categories, according to primary purpose:

- *Support: Supporting controls are generic and underlie most IT security capabilities. These controls must be in place in order to implement other controls. E.g.: Identification, Cryptographic Key Management, Security Administration.*

- *Prevent: Preventive controls focus on preventing security breaches from occurring in the first place. E.g. Authentication., Authorization, Access Control, Enforcement, Non-repudiation, Protected Communications, Transaction Privacy*

- *Detect and Recover: These controls focus on detecting and recovering from a security breach. .e.g. Audit, Intrusion Detection and Containment, Proof of Wholeness, Restore Secure State., Virus Detection and Eradication.*

4.4.2 Management Security Controls:

Management security controls, in conjunction with technical and operational controls, are implemented to manage and reduce the risk of loss and to protect an organization's mission. Management controls focus on the stipulation of information protection policy, guidelines, and standards, which are carried out through operational procedures to fulfill the organization's goals and missions.

4.4.3 Operational Security Controls:

An organization's security standards should establish a set of controls and guidelines to ensure that security procedures governing the use of the organization's IT assets and resources are properly enforced and implemented in accordance with the organization's goals and mission. Management plays a vital role in overseeing policy implementation and in ensuring the establishment of appropriate operational controls. Operational controls, implemented in accordance with a base set of requirements (e.g., technical controls) and good industry practices, are used to correct operational deficiencies that could be exercised by potential threat-sources. To ensure consistency and uniformity in security operations, step-by-step procedures and methods for implementing operational controls must be clearly defined, documented, and maintained.

4.5 Cost-Benefit Analysis:

To allocate resources and implement cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances.

4.6 Residual Risk:

Organizations can analyze the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact, the two parameters that define the mitigated level of risk to the organizational mission. The risk remaining after the implementation of new or enhanced controls is the residual risk. Practically no IT system is risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero.

5. Evaluation and Assessment

In most organizations, the network itself will continually be expanded and updated, its components changed, and its software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving. This section emphasizes the good practice and need for an ongoing risk evaluation and assessment and the factors that will lead to a successful risk management program.

5.1 Good Security Practice

The risk assessment process should usually be repeated at least every 3 years. However, risk management should be conducted and integrated in the SDLC for IT systems, There should be a specific schedule for assessing and mitigating mission risks, but the periodically performed process should also be flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies.

5.2 Keys For Success

A successful risk management program will rely on (1) senior management's commitment; (2) the full support and *participation of the IT team; (3) the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization; (4) the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization; and (5) an ongoing evaluation and assessment of the IT-related mission risks.*

Appendix IV-2-1 (Sample Interview Questions)

Sample Interview Questions

Interview questions should be tailored based upon where the IT system assessed is in the SDLC. Sample questions to be asked during interviews with site personnel to gain an understanding of the operational characteristics of an organization may include the following:

- *Who are valid users?*
- *What is the mission of the user organization?*
- *What is the purpose of the system in relation to the mission?*
- *How important is the system to the user organization's mission?*
- *What is the system-availability requirement?*
- *What information (both incoming and outgoing) is required by the organization?*
- *What information is generated by, consumed by, processed on, stored in, and retrieved by the system?*
- *How important is the information to the user organization's mission?*
- *What are the paths of information flow?*
- *What types of information are processed by and stored on the system (e.g., financial, personnel, research and development, medical, command and control)?*

- *What is the sensitivity (or classification) level of the information?*

- *What information handled by or about the system should not be disclosed and to whom?*

- *Where specifically is the information processed and stored?*

- *What are the types of information storage?*

- *What is the potential impact on the organization if the information is disclosed to unauthorized personnel?*

- *What are the requirements for information availability and integrity?*

- *What is the effect on the organization's mission if the system or information is not reliable?*

- *How much system downtime can the organization tolerate? How does this downtime compare with the mean repair/recovery time? What other processing or communications options can the user access?*

- *Could a system or security malfunction or unavailability result in injury or death?*

Appendix IV-2-2 (Sample Risk Assessment Report Outline)

Sample Risk Assessment Report Outline

EXECUTIVE SUMMARY

I. Introduction

- *Purpose*

- *Scope of this risk assessment*

- *Describe the system components, elements, users, field site locations (if any), and any other details about the system to be considered in the assessment.*

II. Risk Assessment Approach: Briefly describe the approach used to conduct the risk assessment, such as

- *The participants (e.g., risk assessment team members)*
- *The technique used to gather information (e.g., the use of tools, questionnaires)*
- *The development and description of risk scale (e.g., a 3 x 3, 4 x 4, or 5 x 5 risk-level matrix).*

III. System Characterization:

Characterize the system, including hardware (server, router, switch), software (e.g., application, operating system, protocol), system interfaces (e.g., communication link), data, and users. Provide connectivity diagram or system input and output flowchart to delineate the scope of this risk assessment effort.

IV. Threat Statement: Compile and list the potential threat-sources and associated threat actions applicable to the system assessed.

V. Risk Assessment Results: List the observations (vulnerability/threat pairs). Each observation must include

- *Observation number and brief description of observation (e.g., Observation 1: User system passwords can be guessed or cracked)*
- *A discussion of the threat-source and vulnerability pair*
- *Identification of existing mitigating security controls*
- *Likelihood discussion and evaluation (e.g., High, Medium, or Low likelihood)*
- *Impact analysis discussion and evaluation (e.g., High, Medium, or Low impact)*
- *Risk rating based on the risk-level matrix (e.g., High, Medium, or Low risk level)*
- *Recommended controls or alternative options for reducing the risk.*

VI. Summary: Total the number of observations. Summarize the observations, the associated risk levels, the recommendations, and any comments in a table format to facilitate the implementation of recommended controls during the risk mitigation process.

3. Guideline for Use of Cryptography in IAAD

1. Introduction

The Classic definition of Security would list three important Goals of Security: To ensure Confidentiality, Integrity and Availability of Information. Presently, two more goals are increasingly being added to Security Requirement: Authentication, and Non-Repudiation. Authentication is concerned with assuring that a communication is authentic, while non-repudiation prevents either source from denying a transmitted message. Cryptography can play an important role in meeting this requirement

1.1 About Cryptography:

Cryptography is a branch of mathematics based on the transformation of data. Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and the transformation of ciphertext into plaintext by decryption. Cryptography relies upon two basic components: an algorithm (or cryptographic methodology) and a key. The algorithm is the mathematical function used for encryption or decryption, and the key is the parameter used in the transformation.

Cryptography should be considered for data that is sensitive, has a high value, or represents a high value if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. Cryptographic methods provide important functionality to protect against intentional and accidental compromise and alteration of data. These methods support communications security by encrypting the communication prior to transmission and decrypting it at receipt. These methods also provide file/data security by encrypting the data prior to placement on a storage medium and decrypting it after retrieval from the storage medium.

2. Types of Cryptography

There are two basic types of cryptography: secret key systems (also called symmetric systems) and public key systems (also called asymmetric systems). In secret key systems, the same key is used for both encryption and decryption. That is, all parties participating in the communication share a single key. In public key systems, there are two keys: a public key and a private key. The public key used for encryption is different from the private key used for decryption. The two keys are mathematically related, but the private key cannot be determined from the public key.

In general, cryptography is used to meet the following security objectives:

Confidentiality services, restricting access to the content of sensitive data to only those individuals who are authorized to view the data.

Data integrity services, by helping in detection of unauthorized data modifications.

Authentication services, by establishing the validity of a transmission, message, or an originator.

Non-repudiation services, by helping prevent an individual from denying that previous actions had been performed.

2.1 Hardware vs. Software Solutions:

Cryptography can be implemented in hardware, software and/or firmware - each has its related costs and benefits. Historically, software has been less expensive and slower than hardware, although for large applications, hardware may be less expensive. In addition, software is easier to modify or bypass than equivalent hardware products. The advantages of software solutions are in flexibility and portability, ease of use, and ease of upgrade. In many cases, cryptography is implemented in a hardware device but is controlled by software and, therefore, a hybrid solution is provided.

2.2 Public vs. Secret Key Cryptography:

The primary advantage of public-key cryptography is increased security and convenience: private keys never need to be transmitted or revealed to anyone. In a secret-key system, the secret keys must be transmitted (either manually or through a communication channel). There may be a chance that an unauthorized individual can access the secret keys during their transmission. The primary advantage of secret key cryptography is speed. There are popular secret-key encryption methods that are significantly faster than any currently available public-key encryption method. Alternatively, public-key cryptography can be used with secret-key cryptography to get the best of both worlds: the security advantages of public-key systems and the speed advantages of secret key systems. The public-key system can be used to encrypt a secret key that is used to encrypt the bulk of a file or message. The proper management of cryptographic keys is essential to the effective use of cryptography for security. Ultimately, the security of information protected by cryptography directly depends on the protection afforded the keys.

3 Symmetric/Secret Key Cryptography:

This section provides a brief overview of the various Symmetric Key cryptographic methods that are available and being used. As stated earlier, in symmetric key cryptography, the sender and receiver of a message use a shared secret key. The sender uses a secret key to encrypt the message and the receiver uses the same secret key to decrypt the message.

3.1 Data Encryption Standard (DES):

DES is one of the popular Symmetric key encryption methods. It was issued in 1977 by National Bureau of Standards, now National Institute of Standards and Technology (NIST), initially for government use. The cryptographic algorithm in DES is publicly known and converts plaintext to ciphertext using a key that consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, are used for error detection. Selection of a different key causes the cipher that is produced for any given set of inputs to be different. The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data.

The DES standard allows for implementation of the cryptographic algorithm in software, firmware, hardware, or any combination thereof to enable more flexible, cost-effective implementations.

The DES enjoys widespread use. It has also been the subject of much controversy concerning how secure the DES is. The primary concerns were regarding the key size, which at 56 bits was considered not very secure, and the internal structure of the encryption algorithm. It is however the assessment of many that except in areas of extreme sensitivity, the use of DES in commercial applications should not be an immediate cause for concern.

3.2 Triple DES (3DES):

A more secure method for using the DES algorithm in three operations, called Triple DES. The DES standard was revised in 1999 to include Triple DES. The Triple Data Encryption Algorithm (TDEA) modes of operation are used for both enciphering and deciphering operations. These modes are based on threefold compound operations of encryption and decryption using the Data Encryption Algorithm (DEA). If two or three independent keys are used for three DEA operations, it may extend the effective key space of DEA. Three key DES has an effective key length of 168 keys. A number of Internet based applications have adopted three-key triple DES, including PGP and S/MIME.

3.3 International Data Encryption Algorithm:

The International Data Encryption Algorithm (IDEA) is a symmetric encryption algorithm developed by members of the Swiss Federal Institute of Technology. It is one of a number of conventional encryption algorithms that have been proposed in recent years to replace DES. IN terms of adoption, IDEA is one of the most successful of these proposals, and is included in PGP. IDEA uses 128 bit key to encrypt data in blocks of 64 bits. By contrast, DES also uses 64-bit blocks but a 56 bit key. IDEA is designed to facilitate both software and hardware implementation.

3.4 Blowfish:

Blowfish is a symmetric block cipher, with the characteristics of being fast, compact, simple, and ability to provide variable security with key length varying from 32 bits to 448 bits. It is considered by many to be the most formidable conventional *encryption algorithm. It is virtually invulnerable to brute force attack with suitable choice of key length.*

3.5 RC5:

RC5 is a symmetric encryption algorithm developed by Ron Rivest. Some of the special design characteristics of this algorithm include: suitable for hardware and software, fast, variable-length key, low memory requirement, and high security. RC5 is incorporated in many of the commercial products of RSA Data Security. RC5 can encrypt blocks of plaintext of length 32, 64, or 128 bits into blocks of ciphertext of the same length, with key length ranging from 0 to 2040 bits.

3.6 RC2:

RC2 is a symmetric encryption algorithm developed by Ron Rivest. RC2 uses plaintext and ciphertext blocks of 64 bits, and a key size that varies from 8 to 1024 bits. RC2 is used in S/MIME with 40-, 64-, and 128-bit key sizes.

3.7 CAST-128:

CAST is a design procedure for symmetric encryption algorithms developed by Carlisle Adams and Stafford Tavares. CAST-128 makes use of a key size that varies from 40 bits to 128 bits in 8 bit increments. CAST is the result of a long process of research and development and has benefited from extensive reviews by cryptologists. It is beginning to be used in a number of products, including PGP.

3.8 AES (Advanced Encryption Standard):

AES(FIPS-197) is the current US government standard for the algorithm to replace the older DES. This standard is effective from 26th May 2002. A new robust encryption algorithm was needed to replace the aging Data Encryption Standard (FIPS 46-3), which had been developed in the 1970s. In September 1997,NIST issued a Federal Register notice soliciting an unclassified, publicly disclosed encryption algorithm that would be available royalty-free worldwide. Following the submission of 15 candidate algorithms and three publicly held conferences to discuss and analyze the candidates, the field was narrowed to five candidates. NIST continued to study all available information and analyses about the candidate algorithms, and selected one of the algorithms, the Rijndael algorithm, to propose for the AES. Rijndael is a block cipher designed by Joan Daemen and Vincent Rijmen. It works with a 128-bit block size, and key sizes in 128, 192, or 256 bits.

4. Asymmetric Key Cryptography / Public Key Cryptography:

The main problem with symmetric key cryptography is getting the sender and receiver to agree on the secret key without *anyone else finding out. If they are in separate physical locations they must trust a courier, or a phone system, or some other transmission medium to prevent the disclosure of the secret key being communicated.*

The development of Public-key cryptography is said to be the greatest and perhaps only true revolution in the entire history of cryptography. The concept of public-key cryptography was introduced in 1976 by Whitfield Diffie and Martin Hellman [DH76] in order to solve the key management problem. In their approach, each person gets a pair of keys, one called the public key and the other called the private key. Each person's public key is published while the private key is kept secret. All communications involve only public keys, and no private key is ever transmitted or shared. The only requirement is that public keys are associated with their users in a trusted (authenticated) manner. Anyone can send a confidential message by using only the public information, but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient.

Public key algorithms rely on one key for encryption and a different but related key for decryption. These algorithms have the following important characteristics:

o It is computationally infeasible to determine the decryption key given only the knowledge of the cryptographic algorithm and the encryption key.

o Either of the two related keys can be used for encryption, with the other used for decryption.

The following two issues regarding Public key encryption vis-à-vis Symmetric key encryption should be kept in mind:

o There is nothing in principle about either of the two categories of encryption that makes one superior to another from the point of view of resisting cryptanalysis. The security of any encryption scheme would depend on the length of the key, and the computational work involved in breaking a cipher.

o Public key encryption has not made symmetric key encryption obsolete. On the contrary, because of the computational overhead of current public-key encryption schemes, there seems no foreseeable likelihood that conventional encryption will be abandoned. The restriction of public-key cryptography to key management and signature applications is almost universally accepted.

4.1 Applications for Public-key Cryptosystem:

As mentioned in the previous section, Public key systems are characterized by the use of a cryptographic algorithm with two keys, one held private and one available publicly. Depending on the application, the sender uses either the sender's private key, or the receiver's public key, or both, to perform some type of cryptographic function. In broad terms, the use of *public-key cryptosystem falls into three categories:*

1. Encryption/ Decryption:

The sender encrypt's a message with the recipient's public key.

2. Digital Signature:

The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

3. Key Exchange:

two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

4.2 Digital Signatures:

A digital signature is an electronic analogue of a written signature in that the digital signature can be used in proving to the recipient or a third party that the message was, in fact, signed by the originator. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time. Digital signatures authenticate the integrity of the signed data and the identity of the signatory. Digital signatures may also be used in proving to a third party that data was actually signed by the generator of the signature. Digital signatures are intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key which corresponds to, but is not the same as, the private key. Each user possesses a private and public key pair. Anyone can verify the signature of a user by employing that user's public key. Signature generation can be performed only by the possessor of the user's private key. The security of a digital signature system is dependent on maintaining the secrecy of users' private keys. Users must, therefore, guard against the unauthorized acquisition of their private keys. A hash function is used in the signature generation process to obtain a condensed version of data, called a message digest. The message digest is then input to the digital signature (ds) algorithm to generate the digital signature. The digital signature is sent to the intended verifier along with the signed data (often called the message). The verifier of the message and signature verifies the signature by using the sender's public key. The same hash function must also be used in the verification process. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data. A digital signature can also be used to verify that information has not been altered after it was signed; this provides message integrity. The non-repudiation property of a digital signature relies on the mathematical assumption that it is computationally infeasible *to derive the private key from the public key and/or a set of messages and signatures prepared using the private key. The non-repudiation property of a digital signature also relies on the practical assumption that the private key is, or can be, associated with a single entity (the signer), that only the signer has knowledge of or use of the private key, and that the private key can and will be kept secret.*

Digital signatures offer protection not available by alternative signature techniques. One such alternative is a digitized signature. A digitized signature is generated by converting a visual form of a handwritten signature to an electronic image. Although a digitized signature resembles its handwritten counterpart, it does not provide the same protection as a digital signature. Digitized signatures can be forged. They can also be duplicated and appended to other electronic data. Digitized signatures cannot be used to determine if information has been altered after it is signed.

5. Public Key Infrastructure (PKI)

A PKI provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key and are issued by a reliable CA.

The basic components of a PKI are:

- *Public Key Certificate - An electronic record that binds a public key to the identity of the owner of a public-private key pair and is signed by a trusted entity. Public key certificates are the mechanism for describing trust relationships in a PKI. Certificates may be issued to CAs or other end entities. Certificates issued to CAs indicate the certificate holder is trusted to issue additional certificates. Certificates issued to other end entities are appropriate for provisioning other security services, but are not trusted for issuing additional certificates. Certificates include an expiration date. However, if the CA ceases to trust the certificate holder before certificate expiration, the CA must revoke the certificate.*

- *Certificate Revocation List (CRL) - A list of certificates that have been revoked. The list is usually signed by the same entity that issued the certificates. Certificates can be revoked for several reasons. For example, a certificate can be revoked if the owner's private key has been lost; the owner leaves the company/agency; or the owner's name changes. CRLs also provide an important mechanism for documenting the historical revocation status of certificates. That is, a dated signature may be presumed to be valid if the signature date was within the validity period of the certificate, and the current CRL of the issuing CA at that date did not show the certificate to be revoked.*

- *Registration Authority (RA) - An entity that is trusted by the CA to register or vouch for the identity of users to a CA.*

- *Certificate Repository - An electronic site that holds certificates and CRLs. CAs post certificates and CRLs to* *repositories.*

- *Certificate User - An entity that uses certificates to know, with certainty, the public key of another entity.*

- *Certificate Holder - An entity that is issued a certificate and can sign digital documents.*

- *Clients - Entities that validate digital signatures and their certification paths from a known public key of a trusted CA.*

5.1 PKI Architectures

A PKI is often composed of many CAs linked by trust paths. The CAs may be linked in several ways. They may be arranged hierarchically under a "root CA" that issues certificates to subordinate CAs. The CAs can also be arranged independently in a mesh27. Recipients of a signed message with no relationship with the CA that issued the certificate for the sender of the message can still validate the sender's certificate by finding a path between their CA and the one that issued the sender's certificate.

6. Selecting Cryptography - The Process

The process used to select cryptographic methods is similar to the process used to select any IT method. This selection process is documented in the system development life cycle model that contains four phases: planning, definition, acquisition, and operations (including disposal).

Prior to selecting a cryptographic method, one should consider the operational environment, requirements of the application, the types of services that can be provided by each type of cryptography, and the cryptographic objectives that must be met when selecting applicable products.

The following questions should be addressed in determining the appropriate degree of security, including cryptography, which will be required for a system:

- *How critical is the system in meeting the organization's mission?*

- *What are the security/cryptographic objectives required by the system, e.g., integrity, confidentiality?*

- *What regulations and policies are applicable in determining what is to be protected?*

- *What are the threats that are applicable in the environment where the system will be operational?*

- *Are the users knowledgeable about cryptography and how much training will they receive?*

The answers to these questions can be used to formulate a strong developmental approach to integrating cryptographic methods into existing or new systems. A sound approach in integrating cryptographic methods is to develop requirements that are derived from the protection goals and policies for the system. The goals and policies are derived from a risk assessment.

Cryptography is best used when it is designed as an integrated part of the system, rather than as an add-on feature. When this cannot be done, cryptographic functions should be carefully added so that the security that they are intended to provide is not compromised. The least effective approach to implementing cryptography is to immediately begin implementing technical approaches. Implementing technical solutions without determining the requirements is never recommended.

Also, cryptographic methods are intended to address specific security risks and threats. Therefore, implementing only cryptographic methods, and no other security mechanisms in a system, will not necessarily provide adequate security.

By consistently replacing traditional methods, the security and efficiency of a system improves. Benefits from replacing handwritten signatures with electronic or digital signature techniques include reducing the possibility of forgery, reducing administrative processing time, and decreasing the burden of maintaining "traditional" paperwork. A system implementing cryptography will naturally generate new types of documentation, and the cryptographic technology should be applied in handling that documentation.

7. Cryptography in IAAD

This chapter has provided an introduction to Cryptography. Cryptography will increasingly be used in IAAD as computers get networked within the office, and more and more confidential information is moved over unsecured Public Networks like the Internet. All Officers may encrypt the confidential data lying on their Laptops/Desktops using any of the Encryption methods described in this chapter. Confidential e-mails should be digitally signed, and encrypted.