ಅಧ್ಯಾಯ 4

ಯೋಜನೆಯ ಭದ್ರತೆ

4 ಅಧ್ಯಾಯ
ಯೋಜನೆಯ ಭದ್ರತೆ

ಮಾಹಿತಿ ಭದ್ರತೆಯು ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಕಾರ್ಯಾಚರಣೆಯ ಸ್ಥಗಿತ, ದುರುಪಯೋಗ, ಅನಧಿಕೃತ ಬಹಿರಂಗಪಡಿಸುವಿಕೆ, ಮಾರ್ಪಾಡು ಅಥವಾ ಹಾನಿಯ ಅಪಾಯದ ವಿರುದ್ಧ ಮಾಹಿತಿ ಸ್ವತ್ತುಗಳ ರಕ್ಷಣೆಗೆ ಸಂಬಂಧಿಸಿದೆ. ಮಾಹಿತಿಯನ್ನು ಸಂಸ್ಥೆಗಳ ಮೌಲ್ಯಯುತ ಆಸ್ತಿ ಎಂದು ಪರಿಗಣಿಸಲಾಗುತ್ತದೆ ಮತ್ತು ಆದ್ದರಿಂದ ಗೌಪ್ಯತೆ, ಸಮಗ್ರತೆ ಮತ್ತು ಲಭ್ಯತೆಯನ್ನು ಖಾತ್ರಿಪಡಿಸುವ ಮೂಲಕ ರಕ್ಷಿಸಬೇಕಾಗುತ್ತದೆ

4.1 ನೀತಿಗಳನ್ನು ಔಪಚಾರಿಕವಾಗಿ ಅನುಮೋದಿಸಲಾಗಿಲ್ಲ ಮತ್ತು ಅಳವಡಿಸಿಕೊಳ್ಳಲಾಗಿಲ್ಲ

ಒಟ್ಟಾರೆ ಮಾಹಿತಿ ಭದ್ರತಾ ಪರಿಸರಕ್ಕೆ ಸಂಬಂಧಿಸಿದಂತೆ, ಕೆ2 ಯೋಜನೆಯು

(i) ತಾಂತ್ರಿಕ ಸಂಯೋಜಕರ ಜೊತೆಗಿನ ಒಪ್ಪಂದದ ಭಾಗವಾಗಿ ಸೇವಾವಿತರಣೆಗಳಾದ ಮಾಹಿತಿ ಭದ್ರತಾ ನಿರ್ವಹಣಾ ವ್ಯವಸ್ಥೆ, ಮಾಹಿತಿ ಭದ್ರತಾ ನೀತಿ ಮತ್ತು ಮಾಹಿತಿ ಭದ್ರತಾ ಕಾರ್ಯವಿಧಾನ ಇವುಗಳನ್ನು ಅಭಿವೃದ್ಧಿಪಡಿಸಿದೆ.

(ii) ಬ್ಯಾಕ್ ಅಪ್ ಮತ್ತು ದತ್ತಾಂಶ ರಿಟೆನ್ಷನ್ ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಒಳಗೊಂಡಿದೆ

(iii) ವಿಪತ್ತು ಚೇತರಿಕೆ ಯೋಜನೆಯಲ್ಲಿ ನಿಗದಿಪಡಿಸಿದಂತೆ ವ್ಯವಹಾರಗಳ ಮುಂದುವರಿಕೆ ಮತ್ತು ವಿಪತ್ತು ಚೇತರಿಕೆಯನ್ನು ಒಂದೇ ಕಾರ್ಯಚಟುವಟಿಕೆಯಾಗಿ ವಿಲೀನಗೊಳಿಸಿದೆ.

ಕೆ2 ವ್ಯಾಪಾರದ ನಿರಂತರತೆ ಮತ್ತು ವಿಪತ್ತಿನಿಂದ ಚೇತರಿಕೆಯ ಉದ್ದೇಶವನ್ನು ಪೂರೈಸಲು ವಿಪತ್ತು ಚೇತರಿಕೆ ಜಾಲತಾಣವನ್ನು ಸ್ಥಾಪಿಸಿತು. ಭದ್ರತಾ ಮೇಲ್ವಿಚಾರಣೆ ಮತ್ತು ಘಟನೆ ನಿರ್ವಹಣೆಗಾಗಿ ಒಂದು ಭದ್ರತಾ ಕಾರ್ಯಾಚರಣೆ ಕೇಂದ್ರವನ್ನು ಸಹ ಸ್ಥಾಪಿಸಲಾಯಿತು.

ಈ ನೀತಿಗಳನ್ನು ಯೋಜನೆಯಲ್ಲಿ ಬಳಸಲು ಹಿರಿಯ ನಿರ್ವಹಣಾ ತಂಡದಿಂದ ಪರಿಶೀಲಿಸಬೇಕು ಮತ್ತು ಅನುಮೋದಿಸಬೇಕು. ಭದ್ರತಾ ಕಾರ್ಯಚಟುವಟಿಕೆಗಳು, ಗುರುತು ಮತ್ತು ಪ್ರವೇಶ ನಿರ್ವಹಣೆಗೆ ಮಾರ್ಗದರ್ಶನ ನೀಡಲು ತಾಂತ್ರಿಕ ಸಂಯೋಜಕರು ಮತ್ತು ಸಲಹೆಗಾರರು ಸಿದ್ಧಪಡಿಸಿದ ದಾಖಲೆಗಳ ಅನುಮೋದನೆ ಮತ್ತು ಸಮ್ಮತಿಯ ವಿವರಗಳನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಗೆ ಒದಗಿಸಲಿಲ್ಲ.

ತಾಂತ್ರಿಕ ಸಂಯೋಜಕರು ಸಿದ್ಧಪಡಿಸಿದ ದಾಖಲೆಗಳನ್ನು ತಾಂತ್ರಿಕ ಸಮಿತಿ ಸಭೆಗಳಲ್ಲಿ ಪರಿಶೀಲಿಸಲಾಗಿದೆ ಎಂದು ಸರ್ಕಾರವು ಹೇಳಿದೆ (ನವೆಂಬರ್ 2021).

ಯೋಜನೆಯಲ್ಲಿ ಬಳಕೆಗಾಗಿ ದಾಖಲೆಗಳ ಅನುಮೋದನೆ ಮತ್ತು ಸ್ವೀಕಾರದ ಮುದ್ರೆಯನ್ನು ಔಪಚಾರಿಕಗೊಳಿಸಲಾಗಿರಲಿಲ್ಲ ಎಂಬುದು ವಾಸ್ತವವಾಗಿದೆ.

ಸ್ಥಾಪಿತ ನೀತಿಗಳು/ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಅನುಮೋದಿಸಲಾಗಿದೆ ಮತ್ತು ಸ್ಥಳದಲ್ಲಿ ಭದ್ರತಾ ವ್ಯವಸ್ಥೆಯನ್ನು ಹೆಚ್ಚಿಸಲು ನಿಯತಕಾಲಿಕವಾಗಿ ಪರಿಶೀಲಿಸಲಾಗಿದೆ ಎಂದು ಸರ್ಕಾರವು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಬೇಕು.

4.1.1 ಕಾರ್ಯತಂತ್ರದ ನಿಯಂತ್ರಣ ಮಟ್ಟಗಳ ನಿರ್ಣಯ

ಭಾರತ ಸರ್ಕಾರವು ಹೊರಡಿಸಿದ ಮಾರ್ಗಸೂಚಿಗಳು (2010) ಇಲಾಖೆಗಳು ಇ–ಆಡಳಿತ ಯೋಜನೆಗಳ ಮೇಲೆ ಕಾರ್ಯತಂತ್ರದ ನಿಯಂತ್ರಣವನ್ನು ಖಾತ್ರಿಪಡಿಸಿಕೊಳ್ಳಬೇಕೆಂದು ಸೂಚಿಸುತ್ತವೆ, ಇದರಿಂದಾಗಿ ಇಲಾಖೆಯು ಸಾಫ್ಟ್‌ವೇರ್ ಅಪ್ಲಿಕೇಶನ್, ದತ್ತಸಂಚಯಗಳು ಮತ್ತು ಪ್ರಮುಖ ಮೂಲಸೌಕರ್ಯಗಳಂತಹ ಕಾರ್ಯತಂತ್ರದ ಸ್ವತ್ತುಗಳ ಮೇಲೆ ಸಂಪೂರ್ಣ ನಿಯಂತ್ರಣವನ್ನು ಹೊಂದಲು ಮತ್ತು ನಿರ್ಗಮನ ನಿರ್ವಹಣೆ ಸಾಮರ್ಥ್ಯವನ್ನು ಖಚಿತಪಡಿಸಲು ಅನುವಾಗುತ್ತದೆ. ಸಂಸ್ಥೆಗೆ ಸಂಭಾವ್ಯ ಪರಿಣಾಮಗಳ ಆಧಾರದ ಮೇಲೆ ಸಾಫ್ಟ್‌ವೇರ್ ಅಪ್ಲಿಕೇಶನ್‌ನ ಭದ್ರತಾ ವರ್ಗವನ್ನು ವ್ಯಕ್ತಪಡಿಸುವುದನ್ನು ಇದು ಒಳಗೊಂಡಿದೆ. ರಾಷ್ಟ್ರೀಯ ಭದ್ರತೆಗೆ ಒಡ್ಡಿಕೊಳ್ಳುವುದು, ಆಡಳಿತದ ಕೆಲಸದ ಹರಿವಿನ ಸೂಕ್ಷ್ಮತೆ, ದತ್ತಾಂಶ ಮತ್ತು ಮಾಹಿತಿಯ ಕ್ಲಿಷ್ಟತೆ ಮತ್ತು ಹಣಕಾಸಿನ ಲಭ್ಯತೆಯ ಪ್ರಮಾಣ ಇತ್ಯಾದಿ ಗುಣಲಕ್ಷಣಗಳನ್ನು ಪರಿಗಣಿಸಿ ಕಾರ್ಯತಂತ್ರದ ನಿಯಂತ್ರಣ ವರ್ಗವನ್ನು ವ್ಯಾಖ್ಯಾನಿಸಬಹುದು. ಕೆ2 ಯೋಜನೆಯ ಆರ್ ಎಫ್ ಪಿಯು ಕೆ2 ಅಪ್ಲಿಕೇಶನ್, ದತ್ತಸಂಚಯ ಮತ್ತು ನೆಟ್‌ವರ್ಕ್ ಚಟುವಟಿಕೆಗಳ ಪರಿಶೀಲನೆಗಾಗಿ ಸರ್ಕಾರದ ಕಡೆಯ ಭದ್ರತಾ ಆಡಳಿತಗಾರರಿಂದ ಮತ್ತು ಮೂರನೇ ಪರಿಶೋಧಕರೊಬ್ಬರಿಂದ ಕಾರ್ಯತಂತ್ರದ ನಿಯಂತ್ರಣ ಚೌಕಟ್ಟನ್ನು ಸಹ ಕಲ್ಪಿಸಿದೆ.

ಕೆ2ವಿನ ಸೂಕ್ಷ್ಮತೆ ಮತ್ತು ಮಹತ್ವವನ್ನು ನಿರ್ಧರಿಸುವ ಮೂಲಕ ಕೆ2ವಿನ ಕಾರ್ಯತಂತ್ರದ ನಿಯಂತ್ರಣ ಮಟ್ಟವನ್ನು ನಿರ್ಧರಿಸಲಾಗಿಲ್ಲ ಎಂಬುದನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು. ನೈಜ ಸಮಯದಲ್ಲಿ ಭದ್ರತಾ ಬೆದರಿಕೆಗಳು ಅಥವಾ ಘಟನೆಗಳನ್ನು ಗುರುತಿಸಲು, ದಾಖಲಿಸಲು, ವಿಶ್ಲೇಷಿಸಲು ಮತ್ತು ವರದಿ ಮಾಡಲು ಭದ್ರತಾ ಘಟನೆ ನಿರ್ವಹಣಾ ಯೋಜನೆಯನ್ನೂ ಸಹ ಸಿದ್ಧಪಡಿಸಲಾಗಿರಲಿಲ್ಲ.

ಕೆ2 ಕಾರ್ಯತಂತ್ರದ ಚೌಕಟ್ಟಿನ ಭಾಗವಾಗಿ ಕಲ್ಪಿಸಲಾಗಿದ್ದಂತಹ ಭದ್ರತಾ ಆಡಳಿತಗಾರರನ್ನು ನಿಯೋಜಿಸಲಾಗಿಲ್ಲ. ವಿಪತ್ತು ಚೇತರಿಕೆ ಯೋಜನೆಗಳನ್ನು ನಿರ್ದಿಷ್ಟಪಡಿಸಿದ ಚೇತರಿಕೆಯ ಸಮಯ ಮತ್ತು ಉದ್ದೇಶಗಳೊಳಗೆ ತಕ್ಷಣಕ್ಕೆ ಬದಲಾಯಿಸುವ ಸಾಮರ್ಥ್ಯಕ್ಕಾಗಿ ಪರೀಕ್ಷಿಸಿಲ್ಲವಾದ್ದರಿಂದ, ಭದ್ರತಾ ಘಟನೆಗಳಿಗೆ ಪ್ರತಿಕ್ರಿಯಿಸಲು ಕೆ2 ಸಿಸ್ಟಮ್‌ನ ಸಾಮರ್ಥ್ಯವನ್ನು ಪ್ರದರ್ಶಿಸಲಾಗಿರಲಿಲ್ಲ.

4.1.2 ಅಸಮರ್ಪಕ ಭದ್ರತಾ ಲೆಕ್ಕಪರಿಶೋಧನೆ

ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯಿದೆ, 2000ರ ಅನುಚ್ಛೇದ 43ಎ ಮತ್ತು ಅದರ ಅಡಿಯಲ್ಲಿನ ನಿಯಮಗಳು ಕೇಂದ್ರ ಸರ್ಕಾರದಿಂದ ಅನುಮೋದಿಸಲ್ಪಟ್ಟ ಓರ್ವ ಸ್ವತಂತ್ರ ಲೆಕ್ಕಪರಿಶೋಧಕರಿಂದ ಕನಿಷ್ಠ ವರ್ಷಕ್ಕೊಮ್ಮೆ ಅಥವಾ ಮೂಲಸೌಕರ್ಯಗಳ ಗಮನಾರ್ಹ ಉನ್ನತೀಕರಣ ಮಾಡಿದಾಗ ಭದ್ರತಾ ಲೆಕ್ಕಪರಿಶೋಧನೆಯನ್ನು ನಡೆಸುವುದು ಅಗತ್ಯವಾಗಿದೆ. ಅದೇ ರೀತಿ, ದತ್ತಾಂಶ ಸೆಂಟರ್‌ಗಳ ಕುರಿತು ಕೇಂದ್ರ ಸರ್ಕಾರ ಹೊರಡಿಸಿದ ಮಾರ್ಗಸೂಚಿಗಳು ದತ್ತಾಂಶ ಸೆಂಟರ್‌ಗಳ ಭದ್ರತಾ ಸನ್ನದ್ಧತೆಯನ್ನು ನಿಯತಕಾಲಿಕವಾಗಿ (ಆರು ತಿಂಗಳಿಗೊಮ್ಮೆ) ಮೂರನೇ ವ್ಯಕ್ತಿ ಪರಿಣಿತರಿಂದ ಪರಿಶೋಧನೆ ಮಾಡಿಸುವುದನ್ನು ಪ್ರತಿಪಾದಿಸುತ್ತವೆ. ಭದ್ರತಾ ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಅಪ್ಲಿಕೇಶನ್, ಹಾರ್ಡ್‌ವೇರ್, ಸಾಫ್ಟ್‌ವೇರ್ ಮತ್ತು ನೆಟ್‌ವರ್ಕ್ ಘಟಕಗಳು, ಭದ್ರತಾ ನೀತಿಗಳು ಮತ್ತು ಅವುಗಳ ಅನುಷ್ಠಾನ, ನಿರ್ವಹಣಾ ತಂಡವು ನಿರ್ವಹಿಸುವ ಚಟುವಟಿಕೆಗಳ ಪರಿಶೀಲನೆ, ಪ್ರವೇಶ ನಿಯಂತ್ರಣಗಳನ್ನು ಪರಿಶೀಲಿಸುವುದು, ಆರೋಗ್ಯ ತಪಾಸಣೆ ಫಲಿತಾಂಶಗಳನ್ನು ಪರಿಶೀಲಿಸುವುದು, ಸೇವೆಗಳ ಸಮಯವನ್ನು ಪರಿಶೀಲಿಸುವುದು ಇವುಗಳನ್ನು ಒಳಗೊಂಡಿರಬೇಕು. ಅಪ್ಲಿಕೇಶನ್, ನೆಟ್‌ವರ್ಕ್ ಘಟಕಗಳನ್ನು ವ್ಯಾಪಿಸಿದಂತೆ ಕೆ2ವಿನ ಮೂರನೇ ವ್ಯಕ್ತಿ ಭದ್ರತಾ ಪರಿಶೋಧನೆಯನ್ನು ನಿಯತಕಾಲಿಕವಾಗಿ ನಡೆಸಲಾಗಿರಲಿಲ್ಲ ಎಂಬುದನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು.

2015–2021ರ ಅವಧಿಯಲ್ಲಿ ಭದ್ರತಾ ಲೆಕ್ಕಪರಿಶೋಧನೆಗಳನ್ನು ಎಂಟು ಬಾರಿ (ದುರ್ಬಲತೆಯ ಮೌಲ್ಯಮಾಪನ ಮತ್ತು ಒಳನುಸುಳುವ ಪರೀಕ್ಷೆ–3 ಬಾರಿ, ಅಂತರ್ಜಾಲ ಅಪ್ಲಿಕೇಶನ್ ಭದ್ರತೆ–3 ಬಾರಿ,

ಫೈರ್‌ವಾಲ್ ವಿಮರ್ಶೆ–1, ಅಪ್ಲಿಕೇಶನ್‌ನ ಲೆಕ್ಕಪರಿಶೋಧನೆ–1) ನಡೆಸಲಾಗಿದೆ ಎಂದು ಇಲಾಖೆಯು ಹೇಳಿತು. ಭದ್ರತಾ ಲೆಕ್ಕಪರಿಶೋಧನಾ ವರದಿಗಳ ಪರಿಶೀಲನೆಯು ಭದ್ರತಾ ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ವೆಬ್ ಅಪ್ಲಿಕೇಶನ್ ಭದ್ರತೆ, ಒಳನುಸುಳುವ ಪರೀಕ್ಷೆ ಮತ್ತು ದುರ್ಬಲತೆಯ ಮೌಲ್ಯಮಾಪನವನ್ನು ಮಾತ್ರ ಒಳಗೊಂಡಿದ್ದು, ಸಂಪೂರ್ಣ ಅಪ್ಲಿಕೇಶನ್, ನೆಟ್‌ವರ್ಕ್ ಮತ್ತು ದತ್ತಸಂಚಯ ಭದ್ರತಾ ನೀತಿಗಳಾದ ಅಪ್ಲಿಕೇಶನ್ ಕ್ರಿಯಾತ್ಮಕತೆಗಳು, ನೆಟ್‌ವರ್ಕ್ ಘಟಕಗಳು, ಪ್ರವೇಶ ನಿಯಂತ್ರಣಗಳು ಮತ್ತು ದತ್ತಾಂಶ ಸೆಂಟರ್ ಭದ್ರತೆ ಇವುಗಳನ್ನು ಒಳಗೊಂಡಿಲ್ಲ ಎಂಬುದನ್ನು ತೋರಿಸಿದೆ. ಭದ್ರತಾ ಲೆಕ್ಕಪರಿಶೋಧನೆಯ ಆವರ್ತಕತೆ ಮತ್ತು ವ್ಯಾಪ್ತಿಯು ಸಾಕಷ್ಟಿಲ್ಲದ ಕಾರಣ, ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಕೆ2 ಅಪ್ಲಿಕೇಶನ್‌ನ ಭದ್ರತಾ ನಿಯಂತ್ರಣಗಳ ದೃಢತೆಯ ಮೇಲೆ ಭರವಸೆಯನ್ನು ಹೊಂದಲಾಗಲಿಲ್ಲ.

4.2 ಗುರುತು ಮತ್ತು ಪ್ರವೇಶ ನಿರ್ವಹಣೆ

ಗುರುತುನಿರ್ವಹಣೆಯು ಬಳಕೆದಾರರ ಗುರುತುಗಳ (ಐಡಿಗಳು) ಸ್ಥಾಪನೆ ಮತ್ತು ನಿರ್ವಹಣೆ, ಅಧಿಕೃತ ಬಳಕೆದಾರರಿಗೆ ಮಾತ್ರ ಸಿಸ್ಟಮ್‌ಗೆ ಪ್ರವೇಶವನ್ನು ನೀಡಲಾಗುತ್ತದೆ ಎಂಬ ಭರವಸೆಯನ್ನು ಒದಗಿಸಲು ಸಂಬಂಧಿಸಿದ ಧೃಡೀಕರಣ ಮತ್ತು ಮೇಲ್ವಿಚಾರಣೆ ಪ್ರಕ್ರಿಯೆಗಳು ಇವುಗಳನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ. ವಿಶಿಷ್ಟ ಬಳಕೆದಾರ ಗುರುತು ಸಹ ಯಾವುದೇ ಬಳಕೆದಾರರು ಈ ಹಿಂದೆ ನಡೆಸಿದ ಚಟುವಟಿಕೆಯನ್ನು ನಿರಾಕರಿಸುವಂತಿಲ್ಲ ಎಂದು ಖಚಿತಪಡಿಸುತ್ತದೆ, ಅಂದರೆ, ಒಂದು ನಿರ್ದಿಷ್ಟ ಬಳಕೆದಾರರ ಐಡಿಗೆ ನಿಯೋಜಿಸಲಾದ ವ್ಯಕ್ತಿಯನ್ನು ಆ ಐಡಿ ಯೊಂದಿಗೆ ನಿರ್ವಹಿಸಿದ ಚಟುವಟಿಕೆಗೆ ಹೊಣೆಗಾರರನ್ನಾಗಿ ಮಾಡಬಹುದು. ಗುರುತಿಸುವಿಕೆ ಮತ್ತು ನಿರಾಕರಣೆಯನ್ನು ಅಳವಡಿಸಿಕೊಳ್ಳಲು ಕೆ2 ಬಯೋಮೆಟ್ರಿಕ್ಸ್ ಮತ್ತು ಡಿಜಿಟಲ್ ಸಹಿ ಪ್ರಮಾಣಪತ್ರ (ಡಿಎಸ್‌ಸಿ) ಆಧಾರಿತ ದೃಢೀಕರಣ ಕಾರ್ಯವಿಧಾನವನ್ನು ಬಳಸುತ್ತದೆ.

ವಿವಿಧ ವರ್ಗದ ಬಳಕೆದಾರರಿಗೆ ಪ್ರವೇಶವನ್ನು ಅನುಮತಿಸಲು ಕೆ2 ಅನ್ವಯವು ಪಾತ್ರ ಆಧಾರಿತ ಪ್ರವೇಶ ನಿಯಂತ್ರಣ (ಆರ್‌ಬಿಎಸಿ) ಕಾರ್ಯವಿಧಾನವನ್ನು ಬಳಸುತ್ತದೆ. ಇದು ನಿರ್ದಿಷ್ಟ ಪಾತ್ರಗಳಿಗೆ ಅನುಮತಿಗಳು ಮತ್ತು ಸವಲತ್ತುಗಳನ್ನು ಹೊಂದಿಸುವುದು ಮತ್ತು ವಿವಿಧ ಅಧಿಕೃತ ಬಳಕೆದಾರರಿಗೆ ಪಾತ್ರಗಳನ್ನು ನಿಯೋಜಿಸುವುದನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ. ಹೀಗಾಗಿ, ಸಿಸ್ಟಮ್ ಬಳಕೆದಾರರಿಗೆ ಯಾವ ಅನುಮತಿಗಳನ್ನು ನೀಡುತ್ತದೆ ಮತ್ತು ನಿರ್ದಿಷ್ಟ ಸಂಪನ್ಮೂಲಗಳು ಅಥವಾ ಕಾರ್ಯಗಳಿಗೆ ಪ್ರವೇಶವನ್ನು ಮಿತಿಗೊಳಿಸುತ್ತದೆ ಎಂಬುದನ್ನು ಪಾತ್ರವು ನಿರ್ಧರಿಸುತ್ತದೆ.

4.2.1 ಬಯೋಮೆಟ್ರಿಕ್ ಪ್ರವೇಶ

ಪ್ರವೇಶ ನಿಯಂತ್ರಣದ ಭಾಗವಾಗಿ ಕೆ2 ಅನ್ವಯವು ಬಯೋಮೆಟ್ರಿಕ್ ತಂತ್ರಜ್ಞಾನವನ್ನು ಬಳಸಿಕೊಂಡಿತು. ಓರ್ವ ವ್ಯಕ್ತಿಯ ಸಂಗ್ರಹಿತ ಬಯೋಮೆಟ್ರಿಕ್ ಗುಣಲಕ್ಷಣಗಳನ್ನು ಅವಳು/ಅವನು ಹೇಳಿಕೊಳ್ಳುವ ವ್ಯಕ್ತಿಯ ಗುರುತನ್ನು ಪರಿಶೀಲಿಸಲು ಅಧಿಕೃತ ವ್ಯಕ್ತಿಗಳ ದತ್ತಸಂಚಯಕ್ಕೆ ಹೋಲಿಸಲಾಗುತ್ತದೆ. ಓರ್ವ ಕೆ2 ಬಳಕೆದಾರರ ಬಯೋಮೆಟ್ರಿಕ್ ದತ್ತಾಂಶವನ್ನು ಕೆ2 ಒಳಗಿನ ಬಳಕೆದಾರರ ಗುರುತಿಗೆ ಹೋಲಿಕೆ ಮಾಡಬೇಕು ಮತ್ತು ಎರಡೂ ರೀತಿಯ ಯಶಸ್ವಿ ದೃಢೀಕರಣ ಆದ ಮೇಲೆ ಬಳಕೆದಾರರು ಸಿಸ್ಟಮ್‌ಗೆ ಪ್ರವೇಶವನ್ನು ಪಡೆಯುತ್ತಾರೆ.

ಕೆ2ವಿನಲ್ಲಿ ಬಳಸಲಾದ ಬಯೋಮೆಟ್ರಿಕ್ ಸಾಧನದ ತಪ್ಪು ಸ್ವೀಕಾರ ದರ (ಎಫ್‌ಎಆರ್) [19] ಶೇಕಡಾ ಎರಡಕ್ಕಿಂತ ಕಡಿಮೆಯಿದ್ದು ತಪ್ಪು ನಿರಾಕರಣೆ ದರಗಳು (ಎಫ್‌ಆರ್‌ಆರ್) ಶೇಕಡಾ 0.01ರಷ್ಟಿದೆಯೆಂದು ಇಲಾಖೆಯು ಹೇಳಿದೆ. ಆದರೆ, ಬಯೋಮೆಟ್ರಿಕ್ ವ್ಯವಸ್ಥೆಯ ಕಾರ್ಯಕ್ಷಮತೆಯನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಲು ಸ್ಥಾಪಿಸಲಾದ ಕಾರ್ಯವಿಧಾನ, ಬಯೋಮೆಟ್ರಿಕ್ ಉಪ–ವ್ಯವಸ್ಥೆಗೆ ಸಂಬಂಧಿಸಿದಂತೆ ವಿಶ್ಲೇಷಣಾತ್ಮಕ ಮತ್ತು ಮೇಲ್ವಿಚಾರಣಾ ವರದಿಗಳು, ಬಯೋಮೆಟ್ರಿಕ್ ದತ್ತಾಂಶದ ಆಧಾರದ ಮೇಲೆ ನಕಲು

[19] ಎಫ್‌ಎಆರ್ ಮತ್ತು ಎಫ್‌ಆರ್‌ಆರ್ ಬಯೋಮೆಟ್ರಿಕ್ ವ್ಯವಸ್ಥೆಯ ಕಾರ್ಯಕ್ಷಮತೆಯನ್ನು ಅಳೆಯಲು ಪ್ರಾಥಮಿಕ ಅಳತೆಗೋಲುಗಳಾಗಿವೆ.

ಬಳಕೆದಾರರ ಗುರುತಿಸಿದ ವರದಿಗಳು ಲಭ್ಯವಿರಲಿಲ್ಲ. ಸಾಧನಗಳನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಲು ಮತ್ತು ಎಫ್ಎಆರ್ ಮತ್ತು ಎಫ್ಆರ್ಆರ್ ಇವುಗಳು ನಿಗದಿತ ಮಿತಿಗಳಲ್ಲಿವೆ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಈ ವರದಿಗಳು ಮುಖ್ಯವಾಗಿವೆ.

ದಿನನಿತ್ಯದ ಕಾರ್ಯಾಚರಣೆಗಳನ್ನು ನಿರ್ವಹಿಸುವ ಕೆ2 ಅನ್ವಯದ ದೈನಂದಿನ ಬಳಕೆದಾರರು ಬಯೋಮೆಟ್ರಿಕ್ಸ್ನೊಂದಿಗೆ ದೃಢೀಕರಿಸಬೇಕಿತ್ತಾದರೂ ಇಲಾಖೆಯೊಳಗಿನ ಕೆ2 ಬಳಕೆದಾರರು ಬಯೋಮೆಟ್ರಿಕ್ ಗುರುತಿನ ಪ್ರಕ್ರಿಯೆಗೆ ಒಳಗಾಗಿರಲಿಲ್ಲ ಎಂಬುದನ್ನು ಗಮನಿಸಲಾಯಿತು. ಬಯೋಮೆಟ್ರಿಕ್ ದೃಢೀಕರಣ ಪ್ರಕ್ರಿಯೆಯಿಂದ ಇಲಾಖೆಯ ಬಳಕೆದಾರರನ್ನು ಹೊರತು ಪಡಿಸಿರುವುದರಿಂದ ಯೋಜಿತ ದೃಢೀಕರಣ ಕಾರ್ಯವಿಧಾನಗಳಲ್ಲಿ ಲೋಪ ಉಂಟುಮಾಡಿದಂತಾಗಿದೆ.

4.2.2 ಡಿಜಿಟಲ್ ಸಹಿ ಪ್ರಮಾಣಪತ್ರಗಳು

ಕೆ2 ತನ್ನ ಬಳಕೆದಾರ ಗುರುತಿಸುವಿಕೆ ಮತ್ತು ಅಧಿಕೃತತೆಯ ಕಾರ್ಯವಿಧಾನದ ಭಾಗವಾಗಿ ಡಿಜಿಟಲ್ ಸಿಗ್ನೇಚರ್ ಪ್ರಮಾಣಪತ್ರಗಳನ್ನು[20] (ಡಿಎಸ್ಸಿ– ಅಳವಡಿಸಿಕೊಂಡಿದೆ. ಕೆ2 ತನ್ನ ಎಲ್ಲಾ ಬಳಕೆದಾರರಿಗೆ ಡಿಎಸ್ಸಿಗಳನ್ನು ಸಂಗ್ರಹಿಸುತ್ತದೆ ಮತ್ತು ವಿತರಿಸುತ್ತದೆ ಮತ್ತು ಸರ್ಕಾರದ ಇತರ ಇಲಾಖೆಗಳಿಂದ ನೀಡಲಾದ ಡಿಎಸ್ಸಿಗಳನ್ನು ಬಳಸಲು ಅನುಮತಿಸುತ್ತದೆ. ಡಿಎಸ್ಸಿ ಕಾರ್ಯವಿಧಾನದ ನಿರ್ವಹಣೆಯು ಅವುಗಳ ಸಿಂಧುತ್ವವನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡುವುದು, ಅವಧಿ ಮುಗಿಯುವ ಮುನ್ನ ನವೀಕರಣ, ನಿಷ್ಕ್ರಿಯಗೊಂಡ ಡಿಎಸ್ಸಿಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿ ತೆಗೆದುಹಾಕುವುದು, ಮರೆತುಹೋದ ಪಾಸ್ವರ್ಡ್ಗಳಿಗೆ ಪ್ರತಿಕ್ರಿಯಿಸುವುದು ಇತ್ಯಾದಿಗಳನ್ನು ಒಳಗೊಂಡಿದೆ.

4.2.2.1 ಡಿಎಸ್ಸಿಗಳ ನವೀಕರಣದಲ್ಲಿ ವಿಳಂಬ

ಕೆ2ವಿನೊಂದಿಗೆ ಕಾರ್ಯನಿರ್ವಹಿಸುವ ಬಳಕೆದಾರರಿಗೆ ಒಂದು ಮಾನ್ಯವಾದ ಡಿಎಸ್ಸಿಗಳು ಅವಶ್ಯಕವಾಗಿದೆ ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್ ಬಳಕೆಯ ಸುಗಮ ನಿರಂತರತೆಯನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಅವರ ಸಮಯೋಚಿತ ನವೀಕರಣವು ಅತ್ಯಗತ್ಯವಾಗಿರುತ್ತದೆ. ಎಮ್ಡಿಎಮ್ ಮಾಡ್ಯೂಲ್ ಡಿಎಸ್ಸಿ ಮಾಹಿತಿ ಬಳಕೆದಾರ ದೃಢೀಕರಣವನ್ನು ದಾಖಲಿಸುತ್ತದೆ ಮತ್ತು ಬಳಸುತ್ತದೆ. 2017–20ರ ಅವಧಿಯಲ್ಲಿ ನವೀಕರಿಸಲಾದ 16,137 ಡಿಎಸ್ಸಿಗಳ ದತ್ತಾಂಶವನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ವಿಶ್ಲೇಷಿಸಿತು ಮತ್ತು ನವೀಕರಣದಲ್ಲಿ ಒಂದು ದಿನದಿಂದ 1,000 ದಿನಗಳವರೆಗೆ ವಿಳಂಬವಿರುವುದನ್ನು ಗಮನಿಸಲಾಯಿತು. ಏಕೆಂದರೆ ಡಿಎಸ್ಸಿಗಳ ಮುಕ್ತಾಯವನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡುವ ಕಾರ್ಯವಿಧಾನವು ದುರ್ಬಲವಾಗಿತ್ತು ಮತ್ತು ಡಿಎಸ್ಸಿಗಳ ಮಾನ್ಯತೆಯ ಮೇಲೆ ಲಭ್ಯವಿರುವ ಪೂರ್ವ ಮಾಹಿತಿಯ ಆಧಾರದ ಮೇಲೆ ಕೆ2 ಸ್ವಯಂಚಾಲಿತವಾಗಿ ಡಿಎಸ್ಸಿಯ ನವೀಕರಣವನ್ನು ಪ್ರಾರಂಭಿಸುವುದಿಲ್ಲ. ಕಾಲಕಾಲಕ್ಕೆ ಡಿಎಸ್ಸಿಗಳು ಮುಕ್ತಾಯಗೊಳ್ಳುತ್ತಿರುವ ಬಗ್ಗೆ ಸೂಚನೆ ನೀಡದ ಕಾರಣ ಡಿಎಸ್ಸಿಗಳ ಕುರಿತ ಎಮ್ಐಎಸ್ ವರದಿಗಳು ಅಸಮರ್ಪಕವಾಗಿದ್ದವು. ಅವಧಿ ಮುಗಿದ ನಂತರ ಡಿಎಸ್ಸಿಗಳನ್ನು ನವೀಕರಿಸಲು ಬಯಸುವ ಬಳಕೆದಾರರ ನಿದರ್ಶನಗಳನ್ನು ಹೆಲ್ಪ್ಡೆಸ್ಕ್ ದತ್ತಾಂಶ ಸೂಚಿಸುತ್ತದೆ. 617 ಪ್ರಕರಣಗಳಲ್ಲಿ ಡಿಎಸ್ಸಿ ಸಂಬಂಧಿತ ಸಮಸ್ಯೆಗಳನ್ನು ಆಧರಿಸಿ ಇತರ ಬಳಕೆದಾರರಿಗೆ ಹುದ್ದೆಗಳನ್ನು ನಿಯೋಜಿಸಲಾಗಿದೆ

[20] ಡಿಎಸ್ಸಿಗಳು ಭೌತಿಕ ಅಥವಾ ಕಾಗದದ ಪ್ರಮಾಣಪತ್ರಗಳ ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಸ್ವರೂಪವಾಗಿದೆ. ಡಿಎಸ್ಸಿಗಳು ನಿರ್ದಿಷ್ಟ ಉದ್ದೇಶಕ್ಕಾಗಿ ವ್ಯಕ್ತಿಯ ಗುರುತಿನ ಪುರಾವೆಯಾಗಿ ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತವೆ ಮತ್ತು ಒಬ್ಬರ ಗುರುತನ್ನು ಎಲೆಕ್ಟ್ರಾನಿಕ್ ರೂಪದಲ್ಲಿ ಸಾಬೀತುಪಡಿಸಲು, ಮಾಹಿತಿ ಅಥವಾ ಸೇವೆಗಳನ್ನು ಪಡೆಯಲು ಅಥವಾ ದಾಖಲೆಗಳನ್ನು ಡಿಜಿಟಲ್ ಆಗಿ ಸಹಿ ಮಾಡಲು ಬಳಸಬಹುದಾಗಿದೆ. ಡಿಎಸ್ಸಿಗಳನ್ನು ಭಾರತೀಯ ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯ್ದೆ 2000ದ ಸೆಕ್ಷನ್ 24ರ ಅಡಿಯಲ್ಲಿ ಗೊತ್ತುಪಡಿಸಿದ ಪರವಾನಗಿ ಪಡೆದ ಪ್ರಮಾಣೀಕರಣ ಪ್ರಾಧಿಕಾರದಿಂದ (ಸಿಎ) ನೀಡಲಾಗುತ್ತದೆ. ಪ್ರಮಾಣೀಕರಿಸುವ ಪ್ರಾಧಿಕಾರಗಳು ಒಂದರಿಂದ ಮೂರು ವರ್ಷಗಳ ಮಾನ್ಯತೆಯೊಂದಿಗೆ ಡಿಎಸ್ಸಿಗಳನ್ನು ನೀಡಲು ಅಧಿಕಾರ ಹೊಂದಿರುತ್ತವೆ.

ಎಂಬುದನ್ನು ಗಮನಿಸಲಾಯಿತು. ಇದು ಡಿಎಸ್‌ಸಿ ಪ್ರಕ್ರಿಯೆಯಲ್ಲಿ ಇಲಾಖೆಯ ಅಸಮರ್ಥತೆಯನ್ನು ಪ್ರತಿಬಿಂಬಿಸುತ್ತದೆ.

ಡಿಎಸ್‌ಸಿ ಇಲ್ಲದೆ ಕೆ2 ಬಳಕೆದಾರರು ಕೆ2ವಿನಲ್ಲಿ ತಮ್ಮ ಪಾತ್ರಗಳನ್ನು ನಿರ್ವಹಿಸಲು ಸಾಧ್ಯವಾಗುವುದಿಲ್ಲವಾದ್ದರಿಂದ ಇಲಾಖೆಯು ಡಿಎಸ್‌ಸಿಗಳ ಮುಕ್ತಾಯವನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಬೇಕಾಗುತ್ತದೆ ಮತ್ತು ಡಿಎಸ್‌ಸಿಗಳನ್ನು ಸಮಯಕ್ಕೆ ಸರಿಯಾಗಿ ನವೀಕರಿಸಬೇಕು.

ಸಾಮಾನ್ಯವಾಗಿ ಯೋಜನಾ ನಿರ್ವಹಣಾ ಘಟಕದ ಮೂಲಕ ಅರ್ಜಿಯನ್ನು ಸ್ವೀಕರಿಸಿದ ಮೂರು ದಿನಗಳಲ್ಲಿ ಡಿಎಸ್‌ಸಿಗಳನ್ನು ಕೆ2 ಪ್ರಕ್ರಿಯೆಗೊಳಿಸುತ್ತದೆ ಎಂದು ಸರ್ಕಾರವು ಹೇಳಿತು (ನವೆಂಬರ್ 2021). ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಸರ್ಕಾರದ ಪ್ರತಿಕ್ರಿಯೆಯನ್ನು ಅಂಗೀಕರಿಸುತ್ತದೆಯಾದರೂ, ನಿಗದಿತ ಮೂರು ದಿನಗಳ ಅವಧಿಯನ್ನು ಮೀರಿ 1,000 ದಿನಗಳವರೆಗೆ ವಿಳಂಬವಾದ ಉದಾಹರಣೆಗಳಿದ್ದವು ಮತ್ತು ಅಂತಹ ವಿಳಂಬಕ್ಕೆ ಕಾರಣಗಳನ್ನು ವಿಶ್ಲೇಷಿಸಲಾಗಿಲ್ಲ. ಡಿಎಸ್‌ಸಿಗಳಲ್ಲಿನ ಸಮಸ್ಯೆಗಳಿಂದಾಗಿ ಹುದ್ದೆಗಳ ನಿಯೋಗ ಸಂಭವಿಸಿದೆ ಎಂಬುದನ್ನೂ ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿದೆ ಮತ್ತು ಅದನ್ನು ಪರಿಹರಿಸಬೇಕಾಗಿದೆ.

4.2.2.2 ಹಂಚಿಕೆ ಮಾಡಲಾದ ಮತ್ತು ವಾಸ್ತವ ಡಿಎಸ್‌ಸಿಗಳಲ್ಲಿ ವ್ಯತ್ಯಾಸ

ಕೆ2 ನೀಡಲಾಗಿರುವ ಇಲಾಖಾವಾರು 'ಡಿಜಿಟಲ್ ಸಹಿ ಪ್ರಮಾಣಪತ್ರ' ಎಂಬ ಎಮ್‌ಐಎಸ್ ವರದಿಯೊಂದನ್ನು ಒದಗಿಸುತ್ತದೆ. ಈ ವರದಿಯಲ್ಲಿರುವ ಅಂಕಿಅಂಶಗಳು, **ಕೋಷ್ಟಕ 4.1**ರಲ್ಲಿ ತೋರಿಸಿರುವಂತೆ, ಕೆ2 ದತ್ತಸಂಚಯ ಪ್ರಕಾರ ಬಳಕೆಯಲ್ಲಿರುವ ನಿಜವಾದ ಡಿಎಸ್‌ಸಿಗಳೊಂದಿಗೆ ಹೊಂದಿಕೆಯಾಗುತ್ತಿರಲಿಲ್ಲ.

ಕೋಷ್ಟಕ 4.1: ಹಂಚಿಕೆ ಮಾಡಲಾದ ಮತ್ತು ವಾಸ್ತವ ಡಿಎಸ್‌ಸಿಗಳಲ್ಲಿ ವ್ಯತ್ಯಾಸ

ಕ್ರಮ ಸಂಖ್ಯೆ	ಆರ್ಥಿಕ ವರ್ಷ	ನೀಡಲಾಗಿರುವ ಡಿಎಸ್‌ಸಿಗಳ ಸಂಖ್ಯೆ		
		ಎಮ್‌ಐಎಸ್ ವರದಿ ಪ್ರಕಾರ	ದತ್ತಸಂಚಯ ಪ್ರಕಾರ	ವ್ಯತ್ಯಾಸ
1	2014–15	05	24	19
2	2015–16	1,054	2,644	1,590
3	2016–17	2,227	4,719	2,492
4	2017–18	1,373	2,819	1,446
5	2018–19	24,535	21,714	2,821
6	2019–20	13,080	14,065	985
7	2020–21	02	5,468	5,466

ಆಕರ : ಎಮ್‌ಐಎಸ್ ವರದಿಗಳು ಮತ್ತು ದತ್ತಸಂಚಯದ ಮಾಹಿತಿಯ ಅನುಸಾರ

ಅಂಕಿಅಂಶಗಳಲ್ಲಿನ ವ್ಯತ್ಯಾಸವು ದತ್ತಸಂಚಯದ ವಿಶ್ವಾಸಾರ್ಹತೆ ಮತ್ತು ಡಿಎಸ್‌ಸಿಗಳ ನಿರ್ವಹಣೆಯ ಮೇಲಿನ ನಿಯಂತ್ರಣಗಳ ಅನುಪಸ್ಥಿತಿಗೆ ಅನುರೂಪವಾಗಿದೆ. ಇದು ಡಿಎಸ್‌ಸಿಗಳನ್ನು ಬಳಸಿಕೊಂಡು ನಡೆಸಿದ ವಹಿವಾಟಿನ ನೈಜತೆಯ ಮೇಲೆ ಪರಿಣಾಮ ಬೀರಬಹುದಾಗಿದೆ

4.2.2.3 ಡಿಜಿಟಲ್ ಸಹಿಯ ಸಂಕಲ್ಪಿತ ಉದ್ದೇಶಗಳನ್ನು ಸಾಧಿಸಲಾಗಿಲ್ಲ

ಭದ್ರತೆಯ ಅಗತ್ಯತೆಗಳ ಭಾಗವಾಗಿ, ಆರ್‌ಎಫ್‌ಪಿ ಹೇಳುವಂತೆ ಇಲಾಖೆಯು ವ್ಯವಸ್ಥೆಯೊಳಗೆ ಅತ್ಯುನ್ನತ ಮಟ್ಟದ ಸಮಗ್ರತೆ ಮತ್ತು ಜವಾಬ್ದಾರಿ ಹೊಣೆಗಾರಿಕೆಯನ್ನು ನಿರ್ವಹಿಸಲು ಉದ್ದೇಶಿಸಿದೆ ಮತ್ತು ಈ ಉದ್ದೇಶಕ್ಕಾಗಿ ಸಾರ್ವಜನಿಕ ಪ್ರಮುಖ ಮೂಲಸೌಕರ್ಯದ (ಪಿಕೆಐ) ಜೊತೆಗೆ ಬಯೋಮೆಟ್ರಿಕ್ಸ್ ಅನ್ನು ಬಳಸಿಕೊಳ್ಳುವ ಮೂಲಕ ದೃಢೀಕರಣ ಪ್ರಕ್ರಿಯೆಯಲ್ಲಿ ಯಾವುದೇ ಅಸ್ಪಷ್ಟತೆಯನ್ನು ತೆಗೆದುಹಾಕುವ ಅಗತ್ಯವನ್ನು ಪರಿಗಣಿಸುತ್ತದೆ.

ಸಹಿಯನ್ನು ಒಪ್ಪದ ಅಥವಾ ನಿರಾಕರಿಸಿದ ಸಂದರ್ಭದಲ್ಲಿ ಸಹಿ ಮಾಡುವವರು ವಹಿವಾಟಿಗೆ ಸಹಿ ಮಾಡಿದ್ದಾರೆ ಎಂದು ಸಾಬೀತುಪಡಿಸಲು ಇಲಾಖೆಯಲ್ಲಿ ವಿವರಿಸಿದ ಮತ್ತು ದಾಖಲಿತ ಕ್ರಮಗಳ ಅನುಕ್ರಮ ಲಭ್ಯವಿಲ್ಲ ಎಂಬುದನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿದೆ. ಡಿಜಿಟಲ್ ಸಹಿ ಪ್ರಕ್ರಿಯೆಯು ಸ್ವೀಕೃತಿದಾರರ ಹೆಸರು, ಬ್ಯಾಂಕ್ ಖಾತೆ ಸಂಖ್ಯೆ ಇತ್ಯಾದಿ ಸೇರಿದಂತೆ ಸಂಪೂರ್ಣ ವೋಚರ್ ಮಾಹಿತಿಯನ್ನು ಒಳಗೊಂಡಿಲ್ಲ ಎಂಬುದನ್ನು ಗಮನಿಸಲಾಗಿದೆ. 2019–20ರಲ್ಲಿ ಕೈಗೊಂಡ ₹26.74ಕೋಟಿ ಮೊತ್ತವನ್ನು ಒಳಗೊಂಡ 225 ಹಣ ಬಿಡುಗಡೆ ವಹಿವಾಟುಗಳಿಗೆ ಸಂಬಂಧಿಸಿದಂತೆ ಡಿಜಿಟಲ್ ಸಹಿ ಮಾಹಿತಿಯನ್ನು ಸಂಗ್ರಹಿಸುವ ಕ್ಷೇತ್ರಗಳು ಖಾಲಿಯಾಗಿವೆ ಎಂಬುದನ್ನು ಸಹ ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿದೆ.

ಹೀಗಾಗಿ, ಡಿಜಿಟಲ್ ಸಿಗ್ನೇಚರ್ ಪ್ರಕ್ರಿಯೆಯ ಅನುಷ್ಠಾನವು ನಿರಾಕರಣೆ ಮತ್ತು ದತ್ತಾಂಶ ಸಮಗ್ರತೆಯ ಬಗ್ಗೆ ಭರವಸೆ ನೀಡಲು ಸಾಕಷ್ಟಿಲ್ಲವಾಗಿದೆ.

4.3 ವಿಶೇಷಾಧಿಕಾರದ ಖಾತೆಗಳನ್ನು ಸೂಕ್ತವಾಗಿ ನಿರ್ವಹಿಸಲಾಗಿಲ್ಲ

ಮೇಲ್ಪರದ ಬಳಕೆದಾರರ ಖಾತೆಗಳಂತಹ ವಿಶೇಷಾಧಿಕಾರ ಹೊಂದಿದ ಖಾತೆಗಳು ಅವುಗಳ ಆಡಳಿತಾತ್ಮಕ ಪ್ರವೇಶದ ಮಟ್ಟದಿಂದಾಗಿ ಹೆಚ್ಚಿನ ಸಂಭಾವ್ಯ ಅಪಾಯವನ್ನು ಹೊಂದಿವೆ. ಈ ಮೇಲ್ಪರದ ಬಳಕೆದಾರರು ವಾಸ್ತವಿಕವಾಗಿ ಅನಿಯಮಿತ ಸವಲತ್ತುಗಳನ್ನು ಹೊಂದಿರಬಹುದು ಅಥವಾ ಸವಲತ್ತುಗಳನ್ನು ಓದಲು/ಬರೆಯಲು/ಕಾರ್ಯಗತಗೊಳಿಸಲು, ಕಡತಗಳು ಅಥವಾ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ರಚಿಸಲು ಅಥವಾ ಸ್ಥಾಪಿಸಲು, ಕಡತಗಳು ಮತ್ತು ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ಮಾರ್ಪಡಿಸಲು ಮತ್ತು ಬಳಕೆದಾರರು ಮತ್ತು ದತ್ತಾಂಶವನ್ನು ಅಳಿಸಲು ಅನುಮತಿಸುವ ಸಿಸ್ಟಮ್‌ನ ಮಾಲೀಕತ್ವವನ್ನು ಹೊಂದಿರಬಹುದು. ಅವರುಗಳು ಫೈರ್‌ವಾಲ್ ಸಂಯೋಜನೆಗಳನ್ನು ಬದಲಾಯಿಸಲು, ಭದ್ರತಾ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ಬದಲಿಸಲು ಮತ್ತು ಅವರ ಚಟುವಟಿಕೆಯ ಕುರುಹುಗಳನ್ನು ಅಳಿಸಲು ಸಾಧ್ಯವಿದೆ. ಈ ಮೇಲ್ಪರದ ಬಳಕೆದಾರ ಖಾತೆಗಳನ್ನು ರಕ್ಷಿಸಲು ಬಯಸುವ ಸಂಸ್ಥೆಗಳು ಈ ಖಾತೆಗಳನ್ನು ನಿಯಂತ್ರಿಸಲು ಕೆಲವು ನೀತಿಗಳನ್ನು ಜಾರಿಗೆ ತರುತ್ತವೆ ಮತ್ತು ಈ ಸವಲತ್ತು ಹೊಂದಿರುವ ಬಳಕೆದಾರರ ಚಟುವಟಿಕೆಗಳನ್ನು ನಿಯಂತ್ರಿಸಲು ಸಿಸ್ಟಮ್‌ನಲ್ಲಿ ಅಳವಡಿಸಲಾದ ನಿಯಂತ್ರಣಗಳನ್ನು ದಾಖಲಿಸುತ್ತವೆ.

ಇಲಾಖೆಯು ವಿಶೇಷಾಧಿಕಾರದ ಗುರುತು ನಿರ್ವಹಣೆ ಅಥವಾ ವಿಶೇಷಾಧಿಕಾರದ ಪ್ರವೇಶ ನಿರ್ವಹಣೆಗೆ ಕಾರ್ಯವಿಧಾನವನ್ನು ಸ್ಥಾಪಿಸಿರಲಿಲ್ಲ ಅಥವಾ ಅಂತಹ ನೀತಿ ಅಥವಾ ಕಾರ್ಯವಿಧಾನದ ಅಗತ್ಯವನ್ನು ದಾಖಲಿಸಿರಲಿಲ್ಲ.

ಬಳಕೆದಾರರ ಪ್ರವೇಶವನ್ನು ಪರಿಶೀಲಿಸಲು ವಿಶೇಷಾಧಿಕಾರ ಗುರುತು ನಿರ್ವಹಣಾ ಪರಿಹಾರವನ್ನು ನಿಯೋಜಿಸಲು ಪ್ರಸ್ತಾಪಿಸಲಾಗಿದೆ ಎಂದು ಸರ್ಕಾರವು ಹೇಳಿದೆ (ನವೆಂಬರ್ 2021).

ಇಲಾಖೆಯು ಈ ಮೇಲ್ಪರದ ಬಳಕೆದಾರರ ಚಟುವಟಿಕೆಗಳು, ಪಿಎಮ್ಯು ಗೆ/ಕೆ2 ನಿರ್ವಹಣೆಯ ಸೂಕ್ತ ಪ್ರತಿನಿಧಿಗೆ ಈ ಮೇಲ್ಪರದ ಬಳಕೆದಾರರ ಚಟುವಟಿಕೆಯ ನಿಯತಕಾಲಿಕ ವರದಿ ಸಲ್ಲಿಕೆ, ಕರ್ತವ್ಯಗಳ ಹಂಚಿಕೆಯನ್ನು ಜಾರಿಗೊಳಿಸುವ ನೀತಿ, ಪಾಸ್‌ವರ್ಡ್ ನೀತಿ, ಮತ್ತು ಎಲ್ಲಾ ಮೇಲ್ಪರದ ಬಳಕೆ ಅವಧಿಗಳ ಮೇಲ್ವಿಚಾರಣೆ ಮತ್ತು ಪರಿಶೋಧನೆಗಾಗಿ ಇರುವಂತಹ ಪ್ರಕ್ರಿಯೆಗಳು ಇವುಗಳನ್ನು ನಿಯಂತ್ರಿಸಲು ಕಾರ್ಯಚಟುವಟಿಕೆಗಳು ಮತ್ತು ನೀತಿಗಳನ್ನು ಜಾರಿಗೊಳಿಸಬೇಕಾಗಿದೆ.

ಉತ್ಪಾದನಾ ಪರಿಸರದಲ್ಲಿ ಮೇಲ್ಪರದ ಬಳಕೆದಾರರ ಖಾತೆಗಳ ಪ್ರವೇಶ ಮಟ್ಟವನ್ನು ನಿರ್ಣಯಿಸುವ ಅಗತ್ಯವನ್ನು ಕೆ2 ಗುರುತಿಸುತ್ತದೆ ಮತ್ತು ಸೂಕ್ತ ಬಳಕೆಗಾಗಿ ಅವುಗಳನ್ನು ನಿಯತಕಾಲಿಕವಾಗಿ ಪರಿಶೀಲಿಸುತ್ತದೆ ಎಂಬುದನ್ನು ಸರ್ಕಾರವು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಬೇಕಿದೆ.

4.4 ಹೆಲ್ಪ್‌ಡೆಸ್ಕ್‌ನೊಂದಿಗೆ ಬಳಕೆದಾರರ ಪ್ರಮಾಣತೆಗಳ ಹಂಚಿಕೆ

ಹೆಚ್ಚಿನ ಬಳಕೆದಾರರೊಂದಿಗೆ ಹಂಚಿಕೊಂಡ ಖಾತೆಗಳು ಅನಧಿಕೃತ ಪ್ರವೇಶದ ಅಪಾಯವನ್ನು ಹೆಚ್ಚಿಸುತ್ತವೆ. ಕೆ2 ದೃಢೀಕರಣ ವಿಧಾನವಾಗಿ ಸಿಂಗಲ್ ಸೈನ್ ಆನ್(ಎಸ್‌ಎಸ್‌ಓ) ಅನ್ನು ಬಳಸಿಕೊಳ್ಳುತ್ತದೆ. ಈ ಎಸ್‌ಎಸ್‌ಓ

ವಿಧಾನವು ಬಳಕೆದಾರರಿಗೆ ಒಂದೇ ಐಡಿ ಮತ್ತು ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಒಂದೇ ಸಮಯದಲ್ಲಿ ಅನೇಕ ಸಾಫ್ಟ್‌ವೇರ್ ಅಪ್ಲಿಕೇಶನ್ ಸೇವೆಗಳನ್ನು ಪ್ರವೇಶಿಸಲು ಅನುಮತಿಸುತ್ತದೆ. ಇದು ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ನೆನಪಿಟ್ಟುಕೊಳ್ಳುವ ಮತ್ತು ಅನೇಕ ಬಾರಿ ನಮೂದಿಸುವ ಹೊರೆಯನ್ನು ಸುಗಮಗೊಳಿಸುತ್ತದೆ. ಅಂತಹ ವಾತಾವರಣದಲ್ಲಿ, ಪಾಸ್‌ವರ್ಡ್ ಭದ್ರತಾ ದೋಷಗಳಿಗೆ ಒಳಗಾಗುವುದನ್ನು ತಡೆಯಲು ಸಂಸ್ಥೆಯು ತನ್ನ ಉದ್ಯೋಗಿಗಳಲ್ಲಿ ಪಾಸ್‌ವರ್ಡ್ ಹಂಚಿಕೆಯ ಅಭ್ಯಾಸವನ್ನು ತಪ್ಪಿಸುವುದು ಬಹಳ ಮುಖ್ಯವಾಗಿದೆ.

ಕೆಳಕಂಡ ಹೆಲ್ಪ್‌ಡೆಸ್ಕ್ ಚಟುವಟಿಕೆಗಳ ಭಾಗವಾಗಿ ಬಳಕೆದಾರರು ಮತ್ತು ಹೆಲ್ಪ್‌ಡೆಸ್ಕ್ ಪ್ರತಿನಿಧಿಗಳ ನಡುವೆ ಪಾಸ್‌ವರ್ಡ್ ಹಂಚಿಕೆಯ ನಿದರ್ಶನಗಳನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು.

- ದೂರುಗಳನ್ನು ಪರಿಹರಿಸಲು ಬಳಕೆದಾರರ ಪ್ರಮಾಣತೆಗಳನ್ನು (ಬಳಕೆದಾರ ಗುರುತು ಮತ್ತು ಪಾಸ್‌ವರ್ಡ್) ಕೋರಿದ ಹೆಲ್ಪ್‌ಡೆಸ್ಕ್ ತಂಡ
- ಬಳಕೆದಾರರು ತಮ್ಮ ಬಳಕೆದಾರರ ಪ್ರಮಾಣತೆಗಳನ್ನು ಪೋರ್ಟಲ್/ಮೇಲ್ ಮೂಲಕ ಹೆಲ್ಪ್‌ಡೆಸ್ಕ್ ತಂಡಕ್ಕೆ ಹಂಚಿಕೊಂಡಿರುವುದು.

ಬಳಕೆದಾರರ ಪ್ರಮಾಣತೆಗಳನ್ನು ಹೆಲ್ಪ್‌ಡೆಸ್ಕ್‌ನೊಂದಿಗೆ ಹಂಚಿಕೊಳ್ಳುವ ಇಂತಹ ನಿದರ್ಶನಗಳು ಭದ್ರತಾ ಬೆದರಿಕೆಗಳನ್ನು ಒಡ್ಡುತ್ತವೆ.

ತಮ್ಮ ಸ್ವಂತ ರುಜುವಾತುಗಳನ್ನು ಬಳಸಿಕೊಂಡು ಹೆಲ್ಪ್‌ಡೆಸ್ಕ್ ಸಿಬ್ಬಂದಿಗೆ ನಿಯಂತ್ರಿತ ಪ್ರವೇಶವನ್ನು ಒದಗಿಸುವ ಮೂಲಕ ಬಳಕೆದಾರರ ಪ್ರಮಾಣತೆಗಳನ್ನು ರಾಜಿ ಮಾಡಿಕೊಳ್ಳದೆ ಬಳಕೆದಾರರ ಸಮಸ್ಯೆಗಳನ್ನು ಪರಿಹರಿಸುವ ಕಾರ್ಯವಿಧಾನಗಳನ್ನು ಕೆ2 ಸ್ಥಾಪಿಸಬೇಕು. ಬಳಕೆದಾರರ ರುಜುವಾತುಗಳನ್ನು ಬಹಿರಂಗಪಡಿಸುವುದು ಗುರುತಿನ ನಿರ್ವಹಣೆ ಮತ್ತು ನಿರಾಕರಣೆಯ ಮೂಲಭೂತ ತತ್ವಗಳನ್ನು ದುರ್ಬಲಗೊಳಿಸುತ್ತದೆ ಮತ್ತು ಹಣಕಾಸು ನಿರ್ವಹಣಾ ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ಹೆಚ್ಚಿನ ಅಪಾಯದಿಂದ ಕೂಡಿದೆ.

ಇದೊಂದು ಬಳಕೆದಾರರ ಜಾಗೃತಿಯ ವಿಷಯವಾಗಿದೆ ಮತ್ತು ಯಾರೊಂದಿಗೂ ಪ್ರಮಾಣತೆಗಳನ್ನು ಹಂಚಿಕೊಳ್ಳದಂತೆ ಬಳಕೆದಾರರಿಗೆ ಸೂಚಿಸಲಾಗಿದೆ ಎಂದು ಸರ್ಕಾರವು ತಿಳಿಸಿತು (ನವೆಂಬರ್ 2021).

ಇದು ದತ್ತಾಂಶದ ದೃಢೀಕರಣ ಮತ್ತು ನಿರಾಕರಣೆಯ ಮೇಲೆ ಪರಿಣಾಮ ಬೀರುತ್ತದಾದ್ದರಿಂದ ಇಲಾಖೆಯು ಬಳಕೆದಾರರ ಪ್ರಮಾಣತೆಗಳ ಸೂಕ್ಷ್ಮತೆಯನ್ನು ಪರಿಗಣಿಸಿ, ಬಳಕೆದಾರರಲ್ಲಿ ಮತ್ತು ಹೆಲ್ಪ್‌ಡೆಸ್ಕ್ ತಂಡದಲ್ಲಿ ಜಾಗೃತಿ ಮೂಡಿಸುವ ಅಗತ್ಯವಿದೆ ಎಂದು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಅಭಿಪ್ರಾಯಪಟ್ಟಿದೆ.

4.5 ಅಮಾನತುಗೊಂಡ/ನಿವೃತ್ತ ನೌಕರರಿಂದ ವಹಿವಾಟು

ಎಲ್ಲಾ ಉದ್ಯೋಗಿಗಳನ್ನು ಅವರ ಸಂಬಂಧಿತ ಡಿಡಿಓ/ಸಿಓ/ಸಿಸಿಓ ಇವರುಗಳಿಗೆ ಹೊಂದಿಕೆ ಮಾಡಲಾಗಿದೆ. ವರ್ಗಾವಣೆ/ಬಡ್ತಿ/ಅಮಾನತು/ನಿವೃತ್ತಿ/ಮರಣದ ಸಂದರ್ಭದಲ್ಲಿ ಚೆಕ್–ಔಟ್/ಚೆಕ್–ಇನ್ ಪ್ರಕ್ರಿಯೆಯ ಮೂಲಕ ಹಿಂದಿನ ಕಛೇರಿಯಿಂದ ಅವರುಗಳ ಹೊಂದಿಕೆಯನ್ನು ತೆಗೆದುಹಾಕಿ ಹೊಸ ಕಛೇರಿಗೆ ಮರು–ಹೊಂದಿಕೆ ಮಾಡಬೇಕು. ಅಂತಹ ಎಲ್ಲಾ ನಿದರ್ಶನಗಳಲ್ಲಿ, ಡಿಡಿಓ/ಸಿಓ/ಸಿಸಿಓ ಅವರು ಚೆಕ್–ಔಟ್/ಚೆಕ್–ಇನ್ ಮಾಡಲು ಉದ್ಯೋಗಿಯ ಕರ್ನಾಟಕ ಸರ್ಕಾರಿ ವಿಮಾ ಇಲಾಖೆ (ಕೆಜಿಐಡಿ) ಸಂಖ್ಯೆಯೊಂದಿಗೆ ಖಜಾನೆಗೆ ವರದಿ ಮಾಡಬೇಕು. ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತಿರುವ ಅದೇ ಡಿಡಿಓ/ಸಿಓ/ಸಿಸಿಓ ಕಛೇರಿಯೊಳಗೆ ಉದ್ಯೋಗಿಯೊಬ್ಬರನ್ನು ಬಡ್ತಿ/ವರ್ಗಾವಣೆ ಮಾಡಿದಾಗ, ಅವರು ತನ್ನ ಹಳೆಯ ಹುದ್ದೆ/ಪದನಾಮದ ಚೆಕ್–ಔಟ್ ಪ್ರಕ್ರಿಯೆಗೆ ಒಳಗಾಗಬೇಕಾಗುತ್ತದೆ ಮತ್ತು ಅವರ ಹೊಸ ಹುದ್ದೆ/ಪದನಾಮದೊಂದಿಗೆ ಚೆಕ್–ಇನ್ ಮಾಡಬೇಕು. ಬೇರೆ ಡಿಡಿಓ/ಸಿಓ ನಿಂದ ವರ್ಗಾವಣೆಗೊಂಡ ಉದ್ಯೋಗಿ ಆ ಡಿಡಿಓ/ಸಿಓ ನಿಂದ ಚೆಕ್–ಔಟ್ ಆಗಬೇಕು ಮತ್ತು ಅವರು ವರದಿ ಮಾಡಿಕೊಳ್ಳುತ್ತಿರುವ ಹೊಸ ಕಚೇರಿಯಲ್ಲಿ ಚೆಕ್–ಇನ್ ಆಗಬೇಕು ಮತ್ತು ಹೊಸ ಕಚೇರಿಯ ಡಿಡಿಓ/ಸಿಓ/ಸಿಸಿಓ ಅವರು ನೌಕರನ ಡಿಡಿಓ ಕೋಡ್ ಜೊತೆಗೆ ಅವರ ಕೆಜಿಐಡಿ ಸಂಖ್ಯೆಯನ್ನು ಹೊಂದಿಕೆ ಮಾಡಬೇಕು. ಏಕಕಾಲಕ್ಕೆ, ಎಚ್‌ಆರ್‌ಎಮ್‌ಎಸ್‌ನಲ್ಲಿ ಟ್ರಾನ್ಸ್‌ಫರ್–ಔಟ್/ಟ್ರಾನ್ಸ್‌ಫರ್–ಇನ್ ಎಂಬ ಸಮಾನಾಂತರ ಚೆಕ್–ಔಟ್/ಚೆಕ್–ಇನ್ ಪ್ರಕ್ರಿಯೆಯನ್ನು ಕೈಗೊಳ್ಳಬೇಕು.

ಆದಾಗ್ಯೂ, ಅಮಾನತು/ನಿವೃತ್ತಿ/ಸಾವಿನ ಪ್ರಕರಣಗಳಲ್ಲಿ ತೆಗೆದುಕೊಳ್ಳಬೇಕಾದ ಕ್ರಮಗಳನ್ನು ಈ ಪ್ರಕ್ರಿಯೆಯು ಸರಿಯಾಗಿ ವಿವರಿಸುವುದಿಲ್ಲ.

ಮುಂಗಟ್ಟೆ ಪರದೆಗಳು ಮತ್ತು ದತ್ತಸಂಚಯದ ಪರಿಶೋಧನಾ ವಿಶ್ಲೇಷಣೆಯು ಎಚ್‌ಆರ್‌ಎಮ್‌ಎಸ್ ಅಪ್ಲಿಕೇಶನ್ ಕೆ2ವಿನೊಂದಿಗೆ ಸಂಪೂರ್ಣವಾಗಿ ಸಂಯೋಜಿಸಲ್ಪಟ್ಟಿಲ್ಲ ಎಂದು ತೋರಿಸಿತು. ಕೆ2 ಬಳಕೆದಾರರನ್ನು ನೋಂದಾಯಿಸುವಾಗ ಎಚ್‌ಆರ್‌ಎಮ್‌ಎಸ್‌ನಿಂದ ದತ್ತಾಂಶವನ್ನು ಪಡೆಯುತ್ತದೆ. ನೈಜ–ಸಮಯದ ಆಧಾರದ ಮೇಲೆ ದತ್ತಾಂಶವನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಎಚ್‌ಆರ್‌ಎಮ್‌ಎಸ್ ಅಪ್ಲಿಕೇಶನ್‌ನ ಸಂಯೋಜನೆಯಾಗದಿರುವುದು ಬಳಕೆದಾರರ ಪ್ರವೇಶವನ್ನು ನಿರ್ವಹಿಸುವ ಕೆ2 ಸಾಮರ್ಥ್ಯದ ಮೇಲೆ ಪ್ರತಿಕೂಲ ಪರಿಣಾಮ ಬೀರಿತ್ತು. ಇಲಾಖೆಯು ನೌಕರರು ಮತ್ತು ಬಳಕೆದಾರರ ಅಮಾನತು, ವರ್ಗಾವಣೆ ಮುಂತಾದ ಘಟನೆಗಳ ಕುರಿತು ತತ್ಕಾಲೀನ ಸೂಚನೆಗಳನ್ನು ನೀಡಬೇಕು ಮತ್ತು ತಕ್ಷಣಕ್ಕೆ ಅಪ್ಲಿಕೇಶನ್‌ನನ್ನು ಇಂದೀಕರಿಸಬೇಕು.

4.5.1 ಅಮಾನತುಗೊಂಡ ಉದ್ಯೋಗಿಗಳಿಂದ ವಹಿವಾಟುಗಳು

ಎಚ್‌ಆರ್‌ಎಮ್‌ಎಸ್ ಅಪ್ಲಿಕೇಶನ್ ಸರ್ಕಾರಿ ನೌಕರರ ಅಮಾನತು ಮತ್ತು ಹಿಂತೆಗೆದುಕೊಳ್ಳುವಿಕೆ ಎರಡೂ ಘಟನೆಗಳನ್ನೂ ದಾಖಲಿಸುತ್ತದೆ. ಆದರೆ, ಎರಡು ಅಪ್ಲಿಕೇಶನ್‌ಗಳ ನಡುವಿನ ಏಕೀಕರಣವನ್ನು ಇನ್ನೂ ಸಂಪೂರ್ಣವಾಗಿ ಸಾಧಿಸಬೇಕಾಗಿರುವುದರಿಂದ ದತ್ತಾಂಶವನ್ನು ಸ್ವಯಂಚಾಲಿತವಾಗಿ ಇಂದೀಕರಿಸಲಾಗುವುದಿಲ್ಲ. ಕೆ2 ನೌಕರನ (ಅಮಾನತುಗೊಂಡ ಉದ್ಯೋಗಿ) ಅಮಾನತುಗೊಳಿಸುವಿಕೆಯನ್ನು ಆತ ನಿಯೋಜಿಸಲ್ಪಟ್ಟಿದ್ದ ಡಿಡಿಓನೊಂದಿಗೆ ದಾಖಲಿಸುತ್ತದೆ ಮತ್ತು ಆ ಬಳಕೆದಾರರನ್ನು ಅಪ್ಲಿಕೇಶನ್‌ನಲ್ಲಿ ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲು ಅವರ ಕಚೇರಿಗೆ ಸಂಬಂಧಿತ ಖಜಾನೆಗೆ ಪತ್ರದ ಮೂಲಕ ವಿನಂತಿಯೊಂದನ್ನು ಕಳುಹಿಸುತ್ತದೆ. ತದನಂತರ ಉದ್ಯೋಗಿ ವರ್ಗಾವಣೆ/ನಿವೃತ್ತಿ/ಅಮಾನತುಗಾಗಿನ ಮಾಡ್ಯೂಲ್‌ನ ಮೂಲಕ ಉದ್ಯೋಗಿಯನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲಾಗುತ್ತದೆ. ಹುದ್ದೆಗೆ ನೇಮಕ, ನಿಯೋಜನೆ, ನಿವೃತ್ತಿ, ಅಮಾನತು ಈ ಪ್ರತಿಯೊಂದೂ ನಮೂದುಗಳು ಮೂರು–ಹಂತದ ಪರಿಶೀಲನೆ ಕಾರ್ಯವಿಧಾನವನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಸಾಂಸ್ಥಿಕರಚನೆಯ ಸೃಷ್ಟಿಕರ್ತ, ಪರಿಶೀಲಕ ಮತ್ತು ಅನುಮೋದಕರ ಮೂಲಕ ಆಗಬೇಕಾಗುತ್ತದೆ.

ಮುಂಗಟ್ಟೆ ಪರದೆಯ ಪರಿಶೀಲನಾ ವಿಶ್ಲೇಷಣೆಯು, ಅಮಾನತು ದಾಖಲೆಗಳನ್ನು ಸೇರಿಸುವಾಗ ಸಿಸ್ಟಮ್ ಪ್ರತ್ಯೇಕ ಅಧಿಸೂಚನೆ ದಿನಾಂಕ, ಆದೇಶ ಸಂಖ್ಯೆ ಮತ್ತು ಆದೇಶದ ದಿನಾಂಕವನ್ನು ಕೇಳುತ್ತದೆ ಎಂಬುದನ್ನು ತೋರಿಸಿತು. ಮುಂಗಟ್ಟೆ ಪರದೆಯಲ್ಲಿನ 'ಪರಿಣಾಮದ ದಿನಾಂಕ' ಕ್ಷೇತ್ರವನ್ನು ಪ್ರಸ್ತುತ ದಿನಾಂಕಕ್ಕೆ ಸ್ಥಿರೀಕರಿಸಿರುವುದರಿಂದ ಅದನ್ನು ತಿದ್ದಲು ಸಾಧ್ಯವಾಗುವುದಿಲ್ಲ. ಈ ನಮೂದು ಸಾಂಸ್ಥಿಕರಚನೆಯ ಅನುಮೋದಕರಿಂದ ಅಂತಿಮವಾಗಿ ಅನುಮೋದಿಸುವ ಮೊದಲು ಸಾಂಸ್ಥಿಕರಚನೆಯ ಪರಿಶೀಲಕರ ಮೂಲಕ ಸಾಗುತ್ತದೆ. ಇದಲ್ಲದೆ, ಸೂಚನೆಯ ದಿನಾಂಕ ಮತ್ತು ಆದೇಶದ ದಿನಾಂಕವು ಪರಿಣಾಮದ ದಿನಾಂಕಕ್ಕಿಂತ ಮುಂಚೆಯೇ ಇರುವಂತೆ ವ್ಯವಸ್ಥೆಯನ್ನು ವಿನ್ಯಾಸಗೊಳಿಸಲಾಗಿದೆ. ಈ ಬಗ್ಗೆ ಕೆಳಗಿನವುಗಳನ್ನು ಗಮನಿಸಲಾಯಿತು.

- 150 ಬಳಕೆದಾರರು ತಯಾರಕ, ಪರೀಕ್ಷಕ, ಅನುಮೋದಕ ಈ ಎಲ್ಲಾ ಮೂರು ಪಾತ್ರಗಳನ್ನೂ ಹೊಂದಿದ್ದರು ಮತ್ತು 205 ಬಳಕೆದಾರರು ಈ ಪಾತ್ರಗಳಲ್ಲಿ ಕನಿಷ್ಠ ಎರಡು ಪಾತ್ರಗಳನ್ನು ಹೊಂದಿದ್ದರು. ಹೀಗಾಗಿ ಕರ್ತವ್ಯಗಳ ಹಂಚಿಕೆಯ ಕಾರ್ಯವಿಧಾನವನ್ನು ಉಲ್ಲಂಘಿಸಿದಂತಾಗಿದೆ.
- ಸೂಚನೆ ದಿನಾಂಕ ಮತ್ತು ಆದೇಶದ ದಿನಾಂಕಗಳು ಪರಿಣಾಮದ ದಿನಾಂಕದ ನಂತರ ಇದ್ದಂತಹ ಕ್ರಮವಾಗಿ ಮೂರು ಮತ್ತು ಐದು ಪ್ರಕರಣಗಳಿದ್ದವು. ಇದು ಈ ಕ್ಷೇತ್ರಗಳಲ್ಲಿ ಯಾವುದೇ ಧೃಢೀಕರಣಗಳಿಲ್ಲ ಎಂಬುದನ್ನು ಸೂಚಿಸುತ್ತದೆ.

- 22,201 ಪ್ರಕರಣಗಳಲ್ಲಿ ಸೂಚನೆ ದಿನಾಂಕವು ಆದೇಶದ ದಿನಾಂಕಕ್ಕಿಂತ ಹಿಂದಿನದಾಗಿತ್ತು; 4,866 ಪ್ರಕರಣಗಳಲ್ಲಿ ಆದೇಶದ ದಿನಾಂಕವು ಅಧಿಸೂಚನೆ ದಿನಾಂಕಕ್ಕಿಂತ ಹಿಂದಿನದಾಗಿದ್ದವು ಮತ್ತು 17,991 ಪ್ರಕರಣಗಳು ಒಂದೇ ಮೌಲ್ಯವನ್ನು ಹೊಂದಿದ್ದವು.

ಡಿಡಿಓಗಳಿಂದ ವಿನಂತಿಯನ್ನು ಕೆ2 ಮೂಲಕ ಅಲ್ಲದೆ ಮುದ್ರಿತ ರೂಪದಲ್ಲಿ ಕಳುಹಿಸಲಾಗುವುದರಿಂದ ಅಮಾನತು ಮತ್ತು ವಿನಂತಿಯ ದಿನಾಂಕವನ್ನು ಕೆ2ವಿನಲ್ಲಿ ದಾಖಲಿಸಲಾಗುವುದಿಲ್ಲ. 254 ಪ್ರಕರಣಗಳಲ್ಲಿ ಅಮಾನತು ಆದೇಶಗಳಿದ್ದವಾದರೂ ಅದಕ್ಕೆ ಅನುಗುಣವಾದ ರದ್ದತಿ ಆದೇಶಗಳಿರಲಿಲ್ಲ ಮತ್ತು 36 ಪ್ರಕರಣಗಳಲ್ಲಿ ಅಮಾನತು ಹಿಂತೆಗೆದುಕೊಳ್ಳುವ ಆದೇಶಗಳಿದ್ದವಾದರೂ ಅಮಾನತು ಆದೇಶಗಳೇ ಇರಲಿಲ್ಲ. ಒಟ್ಟು 44 ಬಳಕೆದಾರರು ಅಮಾನತು ಮತ್ತು ಹಿಂತೆಗೆದುಕೊಳ್ಳುವ ಆದೇಶಗಳೆಡನ್ನೂ ಹೊಂದಿದ್ದಾರೆಂದು ಕಂಡುಬಂದಿದ್ದು, ಅದರಲ್ಲಿ 10 ಬಳಕೆದಾರರು[21] ₹81.95 ಲಕ್ಷ ಮೌಲ್ಯದ ವಿವಿಧ ಪ್ರಕಾರಗಳ 55 ಬಿಲ್‌ಗಳನ್ನು ಪ್ರಕ್ರಿಯೆಗೊಳಿಸಿದ್ದರು.

ಉದ್ಯೋಗಿ ವರ್ಗಾವಣೆ ಮಾಡ್ಯೂಲ್‌ನ ಮೂಲಕ ಅಮಾನತುಗೊಳಿಸಿದ ಉದ್ಯೋಗಿಗಳ ವರ್ಗಾವಣೆಯನ್ನು ಸಹ ಕೆ2 ಅನುಮತಿಸುತ್ತದೆ. ಅಮಾನತು ಆದೇಶವು ಸಕ್ರಿಯವಾಗಿರುವಾಗಲೂ ವರ್ಗಾವಣೆಗೆ ಅವಕಾಶ ನೀಡಲಾಯಿತು ಎಂದು ಪರಿಶೋಧನಾ ವಿಶ್ಲೇಷಣೆಯು ತೋರಿಸಿತು. ವರ್ಗಾವಣೆ ಪ್ರಕ್ರಿಯೆಯು ಬಳಕೆದಾರರ ಅಮಾನತನ್ನು ಸ್ವಯಂಚಾಲಿತವಾಗಿ ಹಿಂತೆಗೆದುಕೊಳ್ಳುತ್ತದೆ. ಅದನ್ನು ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ಅನುಮತಿಸಬಾರದಾಗಿದೆ. ಅಮಾನತಿನ ನಂತರ ಬಳಕೆದಾರರಿಗೆ ಹುದ್ದೆಗಳನ್ನು ನಿಯೋಜಿಸದೆ ಇರುವುದರಿಂದ ವಹಿವಾಟು ನಡೆಸಲು ಸಾಧ್ಯವಾಗದಿದ್ದರೂ, ಖಜಾನೆ ಬಳಕೆದಾರರು ಈ ಬಳಕೆದಾರರನ್ನು 'ಸಕ್ರಿಯ' ಬಳಕೆದಾರರಂತೆ ನೋಡುವುದರಿಂದ ಅಜಾಗರೂಕತೆಯಿಂದ ಹುದ್ದೆಗಳನ್ನು ನಿಯೋಜಿಸಬಹುದಾಗಿದೆ. ಅಮಾನತುಗೊಂಡ ಬಳಕೆದಾರರನ್ನು ಅಮಾನತು ಹಿಂಪಡೆಯದೆ ವರ್ಗಾವಣೆ ಮಾಡಿರುವ 254 ಪ್ರಕರಣಗಳಿದ್ದವು.

4.5.2 ನಿವೃತ್ತ ಉದ್ಯೋಗಿಗಳಿಂದ ವಹಿವಾಟುಗಳು

ವಯೋನಿವೃತ್ತಿಯ ನಂತರ ಉದ್ಯೋಗಿಗಳ ದಾಖಲೆ ವಿವರಗಳನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲು ಪ್ರತಿ ತಿಂಗಳ ಕೊನೆಯ ದಿನದಂದು ಸಿಸ್ಟಮ್‌ನಲ್ಲಿನ ಲೇಖನವೊಂದನ್ನು ಹಸ್ತಚಾಲಿತವಾಗಿ ಚಾಲನೆ ಮಾಡಲಾಗುತ್ತದೆ. ಪ್ರಸ್ತುತ ದಿನಾಂಕವು ಯಾವುದೇ ಉದ್ಯೋಗಿಯ ಹುಟ್ಟಿದ ದಿನಾಂಕದಿಂದ 60 ವರ್ಷಗಳನ್ನು ಮೀರಿದೆಯೇ ಎಂದು ಲೇಖನವು ಪರಿಶೀಲಿಸುತ್ತದೆ ಮತ್ತು ಲೇಖನದ ಷರತ್ತುಗಳನ್ನು ಪೂರೈಸಿದರೆ, ದಾಖಲೆಯ ಸ್ಥಿತಿಯನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲಾಗುತ್ತದೆ ಮತ್ತು ಸಂಬಂಧಿತ ಕೋಷ್ಟಕಗಳ ನವೀಕರಿಸಿದ ದಿನಾಂಕ ಕ್ಷೇತ್ರದಲ್ಲಿ ಸಿಸ್ಟಮ್ ದಿನಾಂಕವನ್ನು ಸೇರಿಸಲಾಗುತ್ತದೆ ಎಂಬುದನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು (org_user_mst, org_emp_mst, ifms_emp_post_wf_mpg, ifms_emp_mst, org_emp_post_mpg, ifms_employee_details_hrms_mst ಕೋಷ್ಟಕಗಳು). ಆದಾಗ್ಯೂ, ಇದು ತಿಂಗಳ ಮೊದಲ ದಿನದಂದು ಹುಟ್ಟಿದ ಉದ್ಯೋಗಿಯನ್ನು ಹಿಂದಿನ ತಿಂಗಳ ಕೊನೆಯ ದಿನದಂದೇ ನಿವೃತ್ತಿ ಮಾಡುವ ಅಗತ್ಯವನ್ನು ಪರಿಗಣಿಸಿರಲಿಲ್ಲ.

ಉದ್ಯೋಗಿ ಮಾಸ್ಟರ್ ಟೇಬಲ್‌ನ ವಿಶ್ಲೇಷಣೆಯು, ಆಗಸ್ಟ್ 2020ರ ಹೊತ್ತಿಗೆ ಒಟ್ಟು 10,144 ದಾಖಲೆಗಳನ್ನು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿರುವುದು ಕಂಡುಬಂದಿದೆ ಎಂದು ತೋರಿಸಿತು. ಇದರಲ್ಲಿ 8,783 ಬಳಕೆದಾರರನ್ನು ಕಾಲಮಿತಿಯೊಳಗೆ ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲಾಗಿದ್ದರೆ, 1,361 ಬಳಕೆದಾರರನ್ನು ಸರಾಸರಿ 62 ದಿನಗಳ ವಿಳಂಬದೊಂದಿಗೆ ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲಾಗಿತ್ತು. ನಿಷ್ಕ್ರಿಯಗೊಳಿಸುವಿಕೆಯಲ್ಲಿನ ಇಂತಹ ವಿಳಂಬವು ಉದ್ಯೋಗಿಯ ನಿವೃತ್ತಿಯ ನಂತರವೂ ಕೆ2 ಅಪ್ಲಿಕೇಶನ್‌ನ ನಿರಂತರ ಬಳಕೆಗೆ ಕಾರಣವಾಯಿತು ಮತ್ತು

[21] ಲೆಕ್ಕಪರಿಶೋಧನೆಯಲ್ಲಿ, ಅಧಿಸೂಚನೆಯ ದಿನಾಂಕ ಮತ್ತು ಆದೇಶದ ದಿನಾಂಕದ ಇವುಗಳಲ್ಲಿ ಯಾವುದು ನಂತರವೋ ಅದನ್ನು ಅಮಾನತು ದಿನಾಂಕವೆಂದೂ ಮತ್ತು ಎರಡರಲ್ಲಿ ಮೊದಲನೆಯದನ್ನು ಮರುನೇಮಕ ದಿನಾಂಕವೆಂದೂ ಪರಿಗಣಿಸಲಾಗಿದೆ.

166 ಬಳಕೆದಾರರು 4,967 ಬಿಲ್‌ಗಳನ್ನು ₹2,412.15 ಕೋಟಿಗೆ ಅವರು ನಿಷ್ಕ್ರಿಯಗೊಳ್ಳಬೇಕಾದ ದಿನಾಂಕ ಮತ್ತು ನಿಷ್ಕ್ರಿಯಗೊಂಡ ವಾಸ್ತವ ದಿನಾಂಕದ ನಡುವಿನ ಮಧ್ಯಂತರ ಅವಧಿಯಲ್ಲಿ ಪ್ರಕ್ರಿಯೆಗೊಳಿಸಿದ್ದರು.

2,039 ದಾಖಲೆಗಳಲ್ಲಿ, ನಿಷ್ಕ್ರಿಯಗೊಳಿಸುವಿಕೆಯ ದಿನಾಂಕವನ್ನು ಪ್ರತಿನಿಧಿಸುವ ಇಂದೀಕರಣ ದಿನಾಂಕವು ಶೂನ್ಯವಾಗಿದೆ ಎಂಬುದನ್ನು ಗಮನಿಸಲಾಯಿತು. ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲು ಸಿಸ್ಟಮ್ ಕಾರಣಗಳನ್ನು ದಾಖಲಿಸಿರಲಿಲ್ಲ. ಜನ್ಮ ದಿನಾಂಕದ ಆಧಾರದ ಮೇಲೆ ಹೆಚ್ಚಿನ ಪ್ರಕರಣಗಳಲ್ಲಿ ನಿಷ್ಕ್ರಿಯಗೊಳಿಸುವಿಕೆಗೆ ಕಾರಣಗಳನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ನಿರ್ಧರಿಸಬಹುದಾದರೂ, ನೌಕರನ ನಿವೃತ್ತಿ ದಿನಾಂಕದ ಮೊದಲೇ ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲಾದ 802 ದಾಖಲೆಗಳಿಗೆ ಸಂಬಂಧಿಸಿದಂತೆ, ನಿಷ್ಕ್ರಿಯಗೊಳಿಸುವಿಕೆಗೆ ಕಾರಣಗಳನ್ನು ಕೆ2ವಿನಲ್ಲಿ ಲಭ್ಯವಿರುವ ದತ್ತಾಂಶದಿಂದ ಪರಿಶೀಲಿಸಲಾಗಲಿಲ್ಲ.

ತಾತ್ತ್ವಿಕವಾಗಿ, ನಿಷ್ಕ್ರಿಯಗೊಂಡ ಬಳಕೆದಾರರಿಗೆ ವಹಿವಾಟು ನಡೆಸಲು ಅಪ್ಲಿಕೇಶನ್ ಅನುಮತಿಸಬಾರದು. ಬಳಕೆದಾರರು ನಿಷ್ಕ್ರಿಯಗೊಂಡ ನಂತರ ₹154.57 ಕೋಟಿ ಮೊತ್ತದ 4,938 ಬಿಲ್ ವಹಿವಾಟುಗಳನ್ನು ನಿರ್ವಹಿಸಿದ್ದರು ಎಂಬುದನ್ನು ಗಮನಿಸಲಾಯಿತು ಮತ್ತು ಅದರಲ್ಲಿ 3,867 ವಹಿವಾಟುಗಳು 2019–20ರಲ್ಲಿ ನಡೆದಿದ್ದವು. ಎಲ್ಲಾ ಸಂಬಂಧಿತ ಕೋಷ್ಟಕಗಳನ್ನು ಇಂದೀಕರಿಸದ ಕಾರಣದಿಂದಾಗಿ ಇದು ಬಳಕೆದಾರರಿಗೆ ಅಪ್ಲಿಕೇಶನ್‌ಗೆ ಲಾಗಿನ್ ಮಾಡಲು ಅವಕಾಶ ಮಾಡಿಕೊಟ್ಟ ಕಾರಣ ಈ ರೀತಿಯಾಗಿ ಪರಿಣಮಿಸಿತ್ತು.

ನಿದರ್ಶನ

1 ಜೂನ್ 1960ರಂದು ಜನಿಸಿದ ಶ್ರೀ ಸುದರ್ಶನ್ ಕೆ.ಎಸ್, ಸಹಾಯಕ ನಿರ್ದೇಶಕರು, ಶಿಕ್ಷಣ ಇಲಾಖೆ (ಬಳಕೆದಾರರ ಐಡಿ: 1232495467), ಇವರು 31 ಮೇ 2020 ರಂದು ಸೇವೆಯಿಂದ ನಿವೃತ್ತಿ ಹೊಂದಿದರು. ಬಳಕೆದಾರರು ಜುಲೈ 2020ರಲ್ಲಿ ₹4,54,194 ಮೊತ್ತದ 47 ಬಿಲ್‌ಗಳನ್ನು ಪ್ರಕ್ರಿಯೆಗೊಳಿಸಿದ್ದಾರೆ.

ದತ್ತಸಂಚಯದ ವಿನ್ಯಾಸದಲ್ಲಿನ ಸಮಸ್ಯೆಗಳನ್ನು ಸಹ ಗಮನಿಸಲಾಯಿತು. ಸಾಂಸ್ಥಿಕರಚನೆಯ ಉದ್ಯೋಗಿ ಮಾಸ್ಟರ್ ಕೋಷ್ಟಕವು ನೌಕರಿಯಿಂದ ತೆಗೆದುಹಾಕಲಾದ ದಿನಾಂಕ, ಮರಣದ ದಿನಾಂಕ, ರಾಜೀನಾಮೆ ದಿನಾಂಕ ಇವುಗಳನ್ನು ದಾಖಲಿಸಲು ಕ್ಷೇತ್ರಗಳನ್ನು ಒಳಗೊಂಡಿತ್ತಾದರೂ ನಿವೃತ್ತಿಯ ದಿನಾಂಕಕ್ಕೆ ಯಾವುದೇ ಕ್ಷೇತ್ರವಿರಲಿಲ್ಲ. ಸಾಂಸ್ಥಿಕರಚನೆಯ ಬಳಕೆದಾರರ ಮಾಸ್ಟರ್ ಕೋಷ್ಟಕವು ಬಳಕೆದಾರರ ಐಡಿ –1 ಅನ್ನು K-II-ADMIN ಎಂಬ ಬಳಕೆದಾರ ಹೆಸರಿನೊಂದಿಗೆ ಹೊಂದಿತ್ತು ಮತ್ತು ಅದನ್ನು 16 ಜನವರಿ 2018 ರಂದು ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲಾಗಿತ್ತು. ಆದರೆ, ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಿದ ದಿನಾಂಕದ ನಂತರವೂ ಬಳಕೆದಾರರ ಐಡಿ –1 ಮೂಲಕ ಹಲವಾರು ವಹಿವಾಟುಗಳನ್ನು ನಡೆಸಲಾಗಿತ್ತು. ವರ್ಷಾಂತ್ಯದ ವಹಿವಾಟುಗಳ ಲೇಖನದಿಂದ, ಬಿಲ್‌ಗಳನ್ನು ರವಾನೆ ಮಾಡುವ ಮತ್ತು ಸ್ವೀಕರಿಸುವ ಬಳಕೆದಾರರಿಗೆ ಬಳಕೆದಾರರ ಐಡಿ –1 ಅನ್ನು ಸೇರಿಸಲಾಗಿತ್ತು ಮತ್ತು ವರ್ಷಾಂತ್ಯದ ಕೊನೆಯ ದಿನದಂದು ಡಿ–ಆಕ್ಟಿವೇಟ್ ಮಾಡಲಾದ ವಹಿವಾಟುಗಳ ಕ್ಷೇತ್ರಗಳಿಗಾಗಿ ರಚಿಸಲಾಗಿತ್ತು ಮತ್ತು ಇಂದೀಕರಿಸಲಾಗಿತ್ತು ಎಂಬುದನ್ನು ಗಮನಿಸಲಾಯಿತು. ಲೇಖನಗಳು –1 ಅನ್ನು ADMIN ಬಳಕೆದಾರರಾಗಿ ಬಳಸುವುದರಿಂದ, ವಹಿವಾಟುಗಳನ್ನು ಬಳಕೆದಾರ K-II-ADMIN ಇದರಿಂದ ಮಾಡಲಾಗಿದೆಯೇ ಅಥವಾ ಹಿಂಬದಿ ಮೂಲಕ ಇತರ ಲೇಖನಗಳ ಮೂಲಕ ಮಾಡಲಾಗಿದೆಯೇ ಎಂಬುದು ಯಾರಿಗೂ ತಿಳಿಯುವುದೇ ಇಲ್ಲ. ಡಿಡಿಓಗಳಿಗೆ ವೀಕ್ಷಣೆ ಮತ್ತು ಪರಿಶೀಲನೆಗಾಗಿ, ಕೆ2ವಿನ ಒಳಗೆ ಕಚೇರಿಯೊಂದರಲ್ಲಿ ಕೆಲಸ ನಿರ್ವಹಿಸುತ್ತಿರುವ/ನಿವೃತ್ತರಾದ ಉದ್ಯೋಗಿಗಳ ದತ್ತಾಂಶವನ್ನು ಒದಗಿಸುವ ಯಾವುದೇ ವರದಿಯೂ ಇಲ್ಲ.

ವಯೋನಿವೃತ್ತಿಯಂತಹ ತಿಳಿದಿರಬಹುದಾದ ಘಟನೆಗಳ ಬಗ್ಗೆ ಕೆ2ವಿನಲ್ಲಿ ನಿಯಂತ್ರಣಗಳನ್ನು ಸ್ವಯಂಚಾಲಿತಗೊಳಿಸಿ ಮಾಹಿತಿಯ ಸಕಾಲಿಕ ಇಂದೀಕರಣಕ್ಕಾಗಿ ಕಾರ್ಯವಿಧಾನಗಳನ್ನು ಸ್ಥಾಪಿಸಲಾಗಿದೆ ಎಂಬುದನ್ನು ಸರ್ಕಾರವು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಬೇಕು.

4.6 ಬಳಕೆದಾರರ ಅನುಮತಿಗಳನ್ನು ಪರಿಶೀಲಿಸಲಾಗಿಲ್ಲ

ಕೆ2 ನಿಯಮಿತವಾಗಿ ವಿಶೇಷಾಧಿಕಾರಗಳನ್ನು ಮತ್ತು ಸಿಸ್ಟಮ್‌ಗೆ ಪ್ರವೇಶವನ್ನು ಪರಿಶೀಲಿಸುವ ಕಾರ್ಯವಿಧಾನವನ್ನು ಹೊಂದಿರಲಿಲ್ಲ ಅಥವಾ ಬಳಕೆದಾರರ ಪ್ರವೇಶ ಮತ್ತು ಕೆ2 ಬಳಕೆಯ ಎಲ್ಲಾ ಅಂಶಗಳ ಮೇಲೆ ನಿಯಮಿತ ಆಂತರಿಕ ಲೆಕ್ಕಪರಿಶೋಧನೆಯ ಅಗತ್ಯವಿರುವ ಸಿಸ್ಟಂ ಬಳಕೆ ಕಾರ್ಯನೀತಿ ನಿಬಂಧನೆಯನ್ನು ಹೊಂದಿರಲಿಲ್ಲ. ತನ್ನ ಬಳಕೆದಾರರ ಪಾತ್ರಗಳು ಇಲಾಖೆಯ ಕಾರ್ಯಚಟುವಟಿಕೆಗಳು ಮತ್ತು ಉದ್ಯೋಗದ ಪಾತ್ರಗಳಿಗೆ ಸೂಕ್ತವಾಗಿವೆಯೇ ಎಂದು ಪರಿಶೀಲಿಸಲು ಸಹಾಯ ಮಾಡಲು ವರದಿಯನ್ನು ತಯಾರಿಸಲು ಸಿಸ್ಟಮ್‌ಗೆ ಸಾಧ್ಯವಿಲ್ಲ ಎಂಬುದನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು. ಬಳಕೆದಾರರ ಪ್ರವೇಶದ ಪರಿಶೀಲನೆಯ ಅನುಪಸ್ಥಿತಿಯಲ್ಲಿ, ಅನಧಿಕೃತ ಮತ್ತು ಅನುಚಿತ ಪ್ರವೇಶವು ಪತ್ತೆಯಾಗದೆ ಉಳಿಯುವ ಅಪಾಯವು ಹೆಚ್ಚಾಗಿದೆ.

ಕಾನೂನುಬದ್ಧ ಬಳಕೆದಾರರು ಮಾತ್ರ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಅಥವಾ ಮೂಲಸೌಕರ್ಯಗಳಿಗೆ ಪ್ರವೇಶವನ್ನು ಹೊಂದಿದ್ದಾರೆ ಎಂಬುದನ್ನು ಪರಿಶೀಲಿಸಲು ಕೆ2 ಬಳಕೆದಾರರ ಪ್ರವೇಶವನ್ನು ನಿಯತಕಾಲಿಕವಾಗಿ ಪರಿಶೀಲಿಸುತ್ತದೆ ಎಂಬುದನ್ನು ಸರ್ಕಾರವು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಬೇಕು.

4.7 ದತ್ತಾಂಶ ರಕ್ಷಣೆ

ದತ್ತಾಂಶ ರಕ್ಷಣೆಯು ಅಶುದ್ಧಗೊಳ್ಳುವುದು, ತಪ್ಪನುಸರಣೆ ಅಥವಾ ನಷ್ಟದಿಂದ ಪ್ರಮುಖ ಮಾಹಿತಿಯನ್ನು ರಕ್ಷಿಸುವ ಪ್ರಕ್ರಿಯೆಯಾಗಿದೆ. ಇದು ದತ್ತಾಂಶದ ಗೌಪ್ಯತೆ, ಲಭ್ಯತೆ ಮತ್ತು ಸಮಗ್ರತೆಯನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಲು ಬಳಸಲಾಗುವ ತಂತ್ರಗಳು ಮತ್ತು ಪ್ರಕ್ರಿಯೆಗಳ ಒಂದು ಗುಂಪು ಚಟುವಟಿಕೆಯಾಗಿದೆ. ಕೆಲವೊಮ್ಮೆ ಇದನ್ನು ದತ್ತಾಂಶ ಭದ್ರತೆ ಅಥವಾ ಮಾಹಿತಿ ಗೌಪ್ಯತೆ ಎಂದೂ ಕರೆಯಲಾಗುತ್ತದೆ. ಸೂಕ್ಷ್ಮ ದತ್ತಾಂಶವನ್ನು ಸಂಗ್ರಹಿಸುವ, ನಿರ್ವಹಿಸುವ ಅಥವಾ ಸಂಗ್ರಹಿಸುವ ಯಾವುದೇ ಸಂಸ್ಥೆಗೆ ದತ್ತಾಂಶ ರಕ್ಷಣೆ ಕಾರ್ಯತಂತ್ರವು ಅತ್ಯಗತ್ಯವಾಗಿರುತ್ತದೆ. ಒಂದು ಯಶಸ್ವಿ ಕಾರ್ಯತಂತ್ರವು ದತ್ತಾಂಶ ನಷ್ಟ, ಕಳ್ಳತನ ಅಥವಾ ಅಶುದ್ಧಗೊಳ್ಳುವುದನ್ನು ತಡೆಯಲು ಸಹಾಯ ಮಾಡುತ್ತದೆ ಮತ್ತು ಉಲ್ಲಂಘನೆ ಅಥವಾ ವಿಪತ್ತಿನ ಸಂದರ್ಭದಲ್ಲಿ ಉಂಟಾಗುವ ಹಾನಿಯನ್ನು ಕಡಿಮೆ ಮಾಡಲು ಸಹಾಯ ಮಾಡುತ್ತದೆ

4.7.1 ದತ್ತಾಂಶ ಸಂರಕ್ಷಣೆ

ದತ್ತಾಂಶ ವರ್ಗೀಕರಣ ಮತ್ತು ದತ್ತಾಂಶದ ಸಂಭಾವ್ಯ ಅಪಾಯದ ಅಂದಾಜು, ದತ್ತಾಂಶ ಸಂರಕ್ಷಣೆ ಅವಧಿ, ದತ್ತಾಂಶ ಸುರಕ್ಷತೆ ಅಂಶಗಳು, ಸಂರಕ್ಷಣೆ ಅವಧಿ ಮುಗಿದ ನಂತರ ದತ್ತಾಂಶ ವಿಲೇವಾರಿ ಇವುಗಳನ್ನು ಗಮನದಲ್ಲಿರಿಸಿ ಇಲಾಖೆಯು ಸೂಕ್ತವಾದ ದತ್ತಾಂಶ ಸಂರಕ್ಷಣೆ ನೀತಿಯೊಂದನ್ನು (ಡಿಆರ್‌ಟಿಪಿ) ರೂಪಿಸಬೇಕಿತ್ತು ಮತ್ತು ದತ್ತಾಂಶ ಕೇಂದ್ರದ ಸಂರಚನೆಯು ಡಿಆರ್‌ಟಿಪಿ ಯನ್ನು ಬೆಂಬಲಿಸುತ್ತದೆ ಎಂಬುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಬೇಕಿತ್ತು.

ಮಾಸ್ಟರ್ ಸೇವಾ ಒಪ್ಪಂದದ ಅನುಸಾರ, ಸಕ್ರಿಯ ದತ್ತಸಂಚಯದಲ್ಲಿ 10 ವರ್ಷಗಳ ಅವಧಿಗೆ ವಹಿವಾಟಿನ ದತ್ತಾಂಶವನ್ನು ಸಂರಕ್ಷಣೆ ಮಾಡಲು ಇಲಾಖೆಯು ಯೋಜಿಸಿತ್ತು. 10 ವರ್ಷಗಳ ಸಂರಕ್ಷಣೆ ಅವಧಿಯ ಹಿಂದಿನ ಅವಧಿಯ ದತ್ತಾಂಶವನ್ನು ಪ್ರತ್ಯೇಕ ದತ್ತಸಂಚಯದಲ್ಲಿ ಒಟ್ಟುಗೂಡಿಸಲಾದ ರೂಪದಲ್ಲಿ ಇರಿಸಬೇಕಿತ್ತು. ದತ್ತಾಂಶದ ಒಟ್ಟುಗೂಡಿಸುವಿಕೆಯ ಪ್ರಕಾರವನ್ನು ತಾಂತ್ರಿಕ ಸಂಯೋಜಕರು ನಿರ್ಧರಿಸಬೇಕಿತ್ತು ಮತ್ತು ಎಸ್‌ಆರ್‌ಎಸ್ ದಾಖಲೆಯ ಭಾಗವಾಗಿ ದಾಖಲಿಸಬೇಕಿತ್ತು.

ಇದಲ್ಲದೆ, ತಾಂತ್ರಿಕ ಸಂಯೋಜಕರು 10 ವರ್ಷಗಳ ಮೊದಲಿನ ಕಾಲಾಂತರದ ಎಲ್ಲಾ ದತ್ತಾಂಶವನ್ನು ಸಂಗ್ರಹಿಸಿ ಸಂರಕ್ಷಣೆ ಮಾಡಬೇಕಾಗಿತ್ತು ಮತ್ತು ಸಕ್ರಿಯ ದತ್ತಾಂಶ ಬೇಸ್‌ನಿಂದ ಅವುಗಳನ್ನು ತೆಗೆದುಹಾಕಬೇಕಿತ್ತು ಮತ್ತು ಇಲಾಖೆಗೆ ಅಗತ್ಯವಿರುವಾಗ ಮತ್ತು ಅದನ್ನು ಮರುಸ್ಥಾಪಿಸಬೇಕಿತ್ತು.

ಇಲಾಖೆಯು ದತ್ತಾಂಶ ಸಂರಕ್ಷಣೆ ನೀತಿ ಮತ್ತು ಮಾಹಿತಿ ಹಂಚಿಕೆ ನೀತಿಯನ್ನು ಇನ್ನೂ ರೂಪಿಸಿರಲಿಲ್ಲ ಎಂಬುದನ್ನು ಗಮನಿಸಲಾಯಿತು. ದತ್ತಾಂಶ ಸಂರಕ್ಷಣೆ ಮತ್ತು ದತ್ತಾಂಶ ಹಂಚಿಕೆ ನೀತಿಗಳ ಅನುಪಸ್ಥಿತಿಯು

ಕೆ2ವಿನೊಂದಿಗೆ ಲಭ್ಯವಿರುವ ದತ್ತಾಂಶದ ಸಂಭಾವ್ಯ ಬಳಕೆಯನ್ನು ಮತ್ತು ಪ್ರಾಮುಖ್ಯತೆಯನ್ನು ಗುರುತಿಸದಿರುವುದನ್ನು ಸೂಚಿಸುತ್ತದೆ.

ದತ್ತಾಂಶ ಸಂರಕ್ಷಣೆ ನೀತಿಯು ಅಭಿವೃದ್ಧಿ ಹಂತದಲ್ಲಿದೆ ಎಂದು ಸರ್ಕಾರವು ಹೇಳಿತು (ನವೆಂಬರ್ 2021).

4.8 ಭದ್ರತೆ ಮತ್ತು ಘಟನಾವಳಿ ನಿರ್ವಹಣೆ

ಸಂಸ್ಥೆಗಳಿಗೆ ಇತ್ತೀಚಿನ ದಿನಗಳಲ್ಲಿ ಔದ್ಯಮಿಕ ಭದ್ರತೆ ಹೆಚ್ಚು ಮಹತ್ವದ್ದಾಗಿದೆ ಮತ್ತು ಹಣಕಾಸು ಮತ್ತು ಲೆಕ್ಕಪತ್ರ ಮಾಹಿತಿ ವ್ಯವಸ್ಥೆಗಳಿಗೆ ಇದು ಪ್ರಮುಖವಾಗಿದೆ. ಇದು ತಮ್ಮ ಮಾಹಿತಿ ವ್ಯವಸ್ಥೆಯಲ್ಲಿನ ದತ್ತಾಂಶ ಮತ್ತು ಮಾಹಿತಿಯನ್ನು ರಕ್ಷಿಸಲು ಸಂಸ್ಥೆಯು ಅನುಸರಿಸುವ ಪ್ರಕ್ರಿಯೆ ಅಥವಾ ಕ್ರಮಗಳಿಗೆ ಸಂಬಂಧಿಸಿದ್ದಾಗಿದೆ. ಔದ್ಯಮಿಕ ಭದ್ರತಾ ನಿರ್ವಹಣೆಯು ಎಲ್ಲಾ ಸಂಬಂಧಿತ ಅಪಾಯಗಳನ್ನು ಗುರುತಿಸುವುದು, ಅಪಾಯಗಳನ್ನು ನಿರ್ವಹಿಸಲು ಅಗತ್ಯವಿರುವ ನಿಯಂತ್ರಣಗಳು ಮತ್ತು ನಿಯಂತ್ರಣಗಳನ್ನು ಕಾರ್ಯಗತಗೊಳಿಸಲು ಕಾರ್ಯಚಟುವಟಿಕೆ ಸಿದ್ಧಪಡಿಸುವುದನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ. ಆ ಕಾರ್ಯಚಟುವಟಿಕೆಯು ಭದ್ರತಾ ವಿನ್ಯಾಸ ಮತ್ತು ನೀತಿಗಳನ್ನು ಒದಗಿಸಬೇಕು ಮತ್ತು ಭೌತಿಕ ಭದ್ರತಾ ವಿನ್ಯಾಸವನ್ನು ಸ್ಪಷ್ಟಪಡಿಸಬೇಕು.

4.8.1 ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿ ಮೂಲಸೌಕರ್ಯ

ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯಿದೆ, 2000 ಇದು ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿ ಮೂಲಸೌಕರ್ಯವನ್ನು (ಸಿಐಐ) ಕಂಪ್ಯೂಟರ್‌ನ ಒಂದು ಸಂಪನ್ಮೂಲ ಎಂದು ವ್ಯಾಖ್ಯಾನಿಸುತ್ತದೆ. ಅದರ ಅಸಮರ್ಥತೆ ಅಥವಾ ನಾಶವು ರಾಷ್ಟ್ರೀಯ ಭದ್ರತೆ, ಆರ್ಥಿಕತೆ, ಸಾರ್ವಜನಿಕ ಆರೋಗ್ಯ ಅಥವಾ ಸುರಕ್ಷತೆಯ ಮೇಲೆ ದುಷ್ಪರಿಣಾಮವನ್ನು ಬೀರುತ್ತದೆ. ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ (ರಾಷ್ಟ್ರೀಯ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿ ಮೂಲಸೌಕರ್ಯ ಸಂರಕ್ಷಣಾ ಕೇಂದ್ರ[22] ಮತ್ತು ಕಾರ್ಯಗಳು ಮತ್ತು ಕರ್ತವ್ಯಗಳನ್ನು ನಿರ್ವಹಿಸುವ ವಿಧಾನ) ನಿಯಮಗಳು, 2013 ಇದು ನಿಗದಿಪಡಿಸಿರುವಂತೆ ಸಿಐಐ ವ್ಯವಸ್ಥೆಯನ್ನು ರಕ್ಷಿಸುವ ಮೂಲಭೂತ ಜವಾಬ್ದಾರಿಯು ಆ ಸಿಐಐ ನಡೆಸುತ್ತಿರುವ ಸಂಸ್ಥೆಯದೇ ಆಗಿರುತ್ತದೆ.

ರಾಷ್ಟ್ರೀಯ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿ ಮೂಲಸೌಕರ್ಯ ಸಂರಕ್ಷಣಾ ಕೇಂದ್ರವು (ಎನ್‌ಸಿಐಐಪಿಸಿ) ಸರ್ಕಾರವನ್ನು, ಇತರವುಗಳೊಂದಿಗೆ, ಸೂಕ್ಷ್ಮ ವಲಯವೆಂದು ಗುರುತಿಸಿದೆ ಮತ್ತು ದಿನಂಪ್ರತಿ ಒಟ್ಟು ವಹಿವಾಟುಗಳ ಸಂಖ್ಯೆ, ದಿನಂಪ್ರತಿ ಎಲ್ಲಾ ರೀತಿಯ ವಹಿವಾಟುಗಳ ಮೌಲ್ಯ. ಸಂಪರ್ಕಿತ ಸಾಧನಗಳ ಸಂಖ್ಯೆ ಮತ್ತು ನೆಟ್‌ವರ್ಕ್ ಗಾತ್ರ, ವಿವಿಧ ವರ್ಗಗಳ ಗ್ರಾಹಕರ ಸಂಖ್ಯೆ ಇತ್ಯಾದಿ ಮಾನದಂಡಗಳನ್ನು ಆಧರಿಸಿ ಸಿಐಐ ಗಳನ್ನು ಗುರುತಿಸಲು ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ನಿಗದಿಪಡಿಸಿದೆ.

ಮೇಲಿನ ಮಾನದಂಡಗಳನ್ನು ಗಮನದಲ್ಲಿಟ್ಟುಕೊಂಡಲ್ಲಿ, ಕೆ2ವನ್ನು ಸಿಐಐ ಎಂದು ಗುರುತಿಸಲು ಮತ್ತು ಸೂಚಿಸಲು ಅರ್ಹತೆ ಹೊಂದುತ್ತದೆ. ಇಲಾಖೆಯು ವ್ಯವಸ್ಥೆಯ ಸೂಕ್ಷ್ಮತೆಯನ್ನು ಇನ್ನೂ ನಿರ್ಣಯಿಸಬೇಕಾಗಿದೆ ಮತ್ತು ಭಾರತ ಸರ್ಕಾರದ ಮಾರ್ಗಸೂಚಿಗಳ ಅಡಿಯಲ್ಲಿ ಕೆ2ವನ್ನು ಸಿಐಐ ಎಂದು ಸೂಚಿಸಲು ಕ್ರಮಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳಬೇಕಾಗಿದೆ ಎಂಬುದನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು. ಈ ಕೆ2 ಯೋಜನೆಯನ್ನು, ಅದರ ಪ್ರಾಮುಖ್ಯತೆ ಮತ್ತು ನಿರ್ಣಾಯಕತೆಗೆ ಅನುಗುಣವಾಗಿ, ಹೆಚ್ಚಿನ ಭದ್ರತಾ ಮೂಲಸೌಕರ್ಯ ಹೊಂದುವುದರಿಂದ ವಂಚಿಸಿತು. ಕೆ2ವನ್ನು ಸಿಐಐ ಎಂದು ನೇಮಿಸಲು ಕ್ರಮಗಳನ್ನು ಕೈಗೊಳ್ಳುವುದಾಗಿ ಮತ್ತು ಪ್ರಾಮುಖ್ಯತೆಯ ಉನ್ನತ ಸ್ಥಿತಿಗೆ ಅನುಗುಣವಾಗಿ ಮಾಹಿತಿ ಭದ್ರತಾ ನಿಯಂತ್ರಣಗಳನ್ನು ಇರಿಸುವುದಾಗಿ ರಾಜ್ಯ ಸರ್ಕಾರವು ಹೇಳಿತು (ನವೆಂಬರ್ 2021).

[22] ಎನ್‌ಸಿಐಐಪಿಸಿಯು ಭಾರತ ಸರ್ಕಾರದ ಒಂದು ಸಂಸ್ಥೆಯಾಗಿದ್ದು, ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಕಾಯಿದೆ, 2000 ರ ಅನುಚ್ಛೇದ 70A ಅಡಿಯಲ್ಲಿ ರಚಿಸಲಾಗಿದೆ ಮತ್ತು 16 ಜನವರಿ 2014 ದಿನಾಂಕದ ಗೆಜೆಟ್ ಅಧಿಸೂಚನೆ GSR 18(E) ಮೂಲಕ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿ ಮೂಲಸೌಕರ್ಯ ರಕ್ಷಣೆಗಾಗಿ ರಾಷ್ಟ್ರೀಯ ನೋಡಲ್ ಸಂಸ್ಥೆ ಎಂದು ನೇಮಿಸಲಾಗಿದೆ.

4.8.2 ಸ್ವತ್ತು ಮತ್ತು ದಾಸ್ತಾನು ನಿರ್ವಹಣೆ

ಸಿಐಐ ಗಳ ರಕ್ಷಣೆಗಾಗಿ ಎನ್ ಸಿಐಐಪಿಸಿ ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಹೊರತಂದಿದೆ (ಜನವರಿ 2015). ಅದರ ಪ್ರಕಾರ ಸೂಕ್ಷ್ಮ ಸ್ವತ್ತುಗಳ ನಿರ್ವಹಣೆ ಮತ್ತು ಭದ್ರತೆಯಲ್ಲಿ ಒಂದು ಪ್ರಮುಖ ಹಂತವೆಂದರೆ ಸ್ವತ್ತು ಮತ್ತು ದಾಸ್ತಾನು ನಿರ್ವಹಣೆಯಾಗಿದೆ ಮತ್ತು ಇದು ಸಿಐಐ ಗಳ ಒಡೆತನದ ಎಲ್ಲಾ ಭೌತಿಕ ಮತ್ತು ವಾಸ್ತವಿಕ ಸೂಕ್ಷ್ಮ ಸ್ವತ್ತುಗಳಿಗೆ ಸಂಬಂಧಿಸಿದ್ದಾಗಿದೆ. ನಿರ್ವಹಣೆ, ದುರಸ್ತಿ, ಕಳ್ಳತನ ತಡೆಗಟ್ಟುವಿಕೆ, ಸಿಸ್ಟಮ್ ಬಿಲ್ಡ್‌ಗಳನ್ನು ನಿಯಂತ್ರಿಸುವುದು, ನಿಯಮಿತ ಪರಿಶೋಧನೆ/ವಿಮರ್ಶೆಗಳನ್ನು ಕೈಗೊಳ್ಳುವುದು, ದೋಷಪೂರಿತ ವ್ಯವಸ್ಥೆಗಳನ್ನು ಬದಲಾಯಿಸುವುದು ಮತ್ತು ಹಳೆಯ/ದೋಷಪೂರಿತ ವ್ಯವಸ್ಥೆಗಳನ್ನು ತ್ಯಜಿಸುವುದು/ನಾಶಪಡಿಸುವುದು/ ಹರಾಜು ಹಾಕುವುದು ಮುಂತಾದವುಗಳಿಗೆ ಆಸ್ತಿ ದಾಸ್ತಾನು ಮುಖ್ಯವಾಗಿದೆ. ಈ ನಿಯಂತ್ರಣದ ಅನುಪಸ್ಥಿತಿಯು ಸಿಐಐ ಕಾರ್ಯಾಚರಣೆಯಲ್ಲಿ ಮತ್ತು ಮಾಹಿತಿ ಭದ್ರತಾ ನೀತಿಗಳು ಮತ್ತು ಭದ್ರತಾ ನಿಯಂತ್ರಣಗಳ ಅನುಷ್ಠಾನದಲ್ಲಿ ಬಳಸಬೇಕಾದ ಸಾಫ್ಟ್‌ವೇರ್ ಮತ್ತು ಹಾರ್ಡ್‌ವೇರ್‌ಗಳ ಪ್ರವೇಶ ನಿಯಂತ್ರಣ ಪಟ್ಟಿಯನ್ನು ಔಪಚಾರಿಕಗೊಳಿಸಲು ಕಷ್ಟಕರವಾಗಿಸುತ್ತದೆ.

ನಿರ್ವಾಹಕರ ದೃಢೀಕರಣ ಪಡೆದು ಹಾರ್ಡ್‌ವೇರ್ ಮತ್ತು ಸಾಫ್ಟ್‌ವೇರ್ ದಾಸ್ತಾನುಗಳ ಆವರ್ತಕ ಪರಿಶೀಲನೆಯನ್ನು ಖಾತ್ರಿಪಡಿಸಿಕೊಳ್ಳುವುದು, ಉಪಕರಣಗಳು/ಡಿಜಿಟಲ್ ಮಾಧ್ಯಮದ ಚಲನೆಯನ್ನು ಯೋಜನಾ ಮೂಲಸೌಕರ್ಯದಿಂದ/ಕ್ಕೆ ವಿಶೇಷವಾಗಿ ಸೂಕ್ಷ್ಮ ಸಂವೇದಿ ಪ್ರದೇಶಗಳನ್ನು ಸಮರ್ಪಕವಾಗಿ ನಿಯಂತ್ರಿಸುವುದು ಮತ್ತು ದಾಸ್ತಾನುಗಳನ್ನು ಇಂದೀಕರಿಸಿದ ನಂತರ ಪಡೆದ ನಂತರ ಸ್ವತ್ತುಗಳನ್ನು ತ್ಯಜಿಸುವುದು/ಬದಲಿಸುವುದು/ಹರಾಜು ಹಾಕುವುದು ಇವುಗಳು ಉತ್ತಮ ಸದಭ್ಯಾಸಗಳಾಗಿವೆ.

ಪ್ರತಿ ಖಜಾನೆ ಕಚೇರಿಯಲ್ಲಿನ ಐಟಿ ಮೂಲಸೌಕರ್ಯಗಳ ಪರಿಶೀಲನೆಯನ್ನು ನಿಯತಕಾಲಿಕವಾಗಿ ತಪಾಸಣಾ ತಂಡಗಳು ಮಾಡುತ್ತವೆ ಎಂದು ಸರ್ಕಾರವು ಹೇಳಿತು (ನವೆಂಬರ್ 2021). ಪ್ರತಿ ಖಜಾನೆ ಕಚೇರಿಯಲ್ಲಿ ಪ್ರವೇಶ ಮತ್ತು ನಿರ್ಗಮನದ ಸಮಯದಲ್ಲಿ ಐಟಿ ಮೂಲಸೌಕರ್ಯದ ಚಲನೆಯನ್ನು ದಾಸ್ತಾನು ಪುಸ್ತಕದಲ್ಲಿ ದಾಖಲಿಸಲಾಗುತ್ತದೆ.

ಆದಾಗ್ಯೂ, ಇಲಾಖೆಯು ನಿರ್ವಹಿಸಿದ ದಾಸ್ತಾನು ಪುಸ್ತಕಗಳನ್ನು ಮತ್ತು ಈ ಸ್ವತ್ತುಗಳಿಗೆ ಸಂಬಂಧಿಸಿದಂತೆ ಕಾಲಕಾಲಕ್ಕೆ ನಡೆಸಲಾದ ದಾಸ್ತಾನು ಪರಿಶೀಲನೆ ಸಂಬಂಧಿತ ವರದಿಗಳನ್ನು ಒದಗಿಸಲಿಲ್ಲ. ಆದ್ದರಿಂದ, ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಈ ದಾಖಲೆಗಳ ನಿಖರತೆ ಮತ್ತು ಸಂಪೂರ್ಣತೆ ಮತ್ತು ಅವುಗಳ ಭೌತಿಕ ಲಭ್ಯತೆಯ ಬಗ್ಗೆ ಭರವಸೆ ಹೊಂದಲು ಸಾಧ್ಯವಾಗಲಿಲ್ಲ.

4.8.3 ಭದ್ರತಾ ದುರ್ಬಲತೆಗಳು

4.8.3.1 ಸರ್ವರ್ ಗಟ್ಟಿತನ ಮತ್ತು ದತ್ತಸಂಚಯ ಬಳಕೆದಾರ ಐಡಿ ಮತ್ತು ಪಾಸ್‌ವರ್ಡ್ ಬಹಿರಂಗಪಡಿಸುವುದು

ವರದಿಗಳನ್ನು ರಚಿಸಲು ಕೆ2 ಜಾಸ್ಪರ್–ಸಾಫ್ಟ್ ಸರ್ವರ್ ಅನ್ನು ಬಳಸುತ್ತದೆ. ಜಾಸ್ಪರ್ ಸರ್ವರ್‌ನ ಬಳಕೆಯ ಪರಿಶೀಲನಾ ವಿಶ್ಲೇಷಣೆಯು ಇದನ್ನು ನಿಯೋಜಿತ ನಿರ್ವಾಹಕರ ಲಾಗಿನ್ ಪ್ರಮಾಣತೆಗಳೊಂದಿಗೆ (ಬಳಕೆದಾರ ಹೆಸರು jasper-admin ಮತ್ತು ನಿಯೋಜಿತ ಪಾಸ್‌ವರ್ಡ್ jasper-admin) ಸ್ಥಾಪಿಸಲಾಗಿದೆ ಎಂದು ತೋರಿಸಿತು. ಪರಿಣಾಮವಾಗಿ, ಯಾವುದೇ ಆಡಳಿತೇತರ ಕೆ2 ಬಳಕೆದಾರರು ಈ ಪ್ರಮಾಣತೆಗಳನ್ನು ಬಳಸಿಕೊಂಡು ನಿರ್ವಾಹಕರಾಗಿ ಜಾಸ್ಪರ್ ಸರ್ವರ್‌ಗೆ ಲಾಗ್ ಇನ್ ಮಾಡಬಹುದಾಗಿದೆ. ಅಂತಹ ಲಾಗಿನ್‌ಗಳ ಮೂಲಕ, ವರದಿ ಫೈಲ್‌ಗಳನ್ನು ಅಳಿಸಿ ಹಾಕುವುದು, ವರದಿಯ ವಿನ್ಯಾಸವನ್ನು ತಿದ್ದಿ ತಪ್ಪಾದ ವರದಿ ಇತ್ಯಾದಿಗಳಿಗೆ ಕಾರಣವಾಗಬಹುದಾದ್ದರಿಂದ, ನಿರ್ವಾಹಕರ ಲಾಗಿನ್‌ನ ಸವಲತ್ತುಗಳನ್ನು ದುರುಪಯೋಗಪಡಿಸಿಕೊಳ್ಳುವ ಸಾಧ್ಯತೆಯಿದೆ.

ಅಲ್ಲದೆ, ಜಾಸ್ಪರ್ ಸರ್ವರ್ ವರದಿ ಉತ್ಪಾದನೆಯ ಸಾಧನವಾಗಿದೆ, ಇದು ದತ್ತಾಂಶವನ್ನು ಪ್ರಶ್ನಿಸಲು ಮತ್ತು ಹಿಂಪಡೆಯಲು ಅಗತ್ಯವಿದೆ. ಆದ್ದರಿಂದ, ಉತ್ಪಾದನಾ ದತ್ತಸಂಚಯವನ್ನು ಪ್ರವೇಶಿಸಲು ಇದು

ಪ್ರಮಾಣತೆಗಳೊಂದಿಗೆ ಜೋಡಣೆ ಹೊಂದಿರಬೇಕು. ಜಾಸ್ಪರ್ ಸರ್ವರ್ ನಿರ್ವಾಹಕರ ಲಾಗಿನ್‌ಗಾಗಿನ ನಿಯೋಜಿತ ಪ್ರಮಾಣತೆಗಳು ಯಾವುದೇ ಕೆ2 ಬಳಕೆದಾರರಿಗೆ ಪ್ರಮಾಣತೆಗಳನ್ನು ಕಲಿತು ಉತ್ಪಾದನಾ ದತ್ತಸಂಚಯವನ್ನು ಪ್ರವೇಶಿಸಲು ಅನುವು ಮಾಡಿಕೊಡುತ್ತವೆ. ಇದು ಉತ್ಪಾದನಾ ದತ್ತಸಂಚಯದ ಪಾಸ್‌ವರ್ಡ್ ಗೌಪ್ಯತೆಯನ್ನು ಶೂನ್ಯಗೊಳಿಸುತ್ತದೆ.

ಕೆ2ವಿನ ಜಂಟಿ ನಿರ್ದೇಶಕರು ಮತ್ತು ಹೆಚ್ಚುವರಿ ನಿರ್ದೇಶಕರು ಇವರುಗಳು ದತ್ತಸಂಚಯ ಅನ್ನು ಪ್ರವೇಶಿಸಲು ಸರ್ವರ್‌ನಲ್ಲಿ ದಾಖಲಿಸಲಾದ ಪ್ರಮಾಣತೆಗಳನ್ನು ಬಹಿರಂಗಪಡಿಸುವ ಮೂಲಕ ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಜಾಸ್ಪರ್ ಸರ್ವರ್‌ನ ಸರ್ವರ್ ಗಟ್ಟಿತನ ಕಳಪೆಯಾಗಿರುವುದನ್ನು ರುಜುವಾತುಪಡಿಸಿತು (9 ಸೆಪ್ಟೆಂಬರ್ 2020).

ಜಾಸ್ಪರ್ ಸರ್ವರ್ ಅನ್ನು 'ಓದಲು ಮಾತ್ರ' ಪ್ರವೇಶದೊಂದಿಗೆ ನಿರ್ಬಂಧಿತ ಬಳಕೆದಾರ ಖಾತೆಯ ಬದಲಿಗೆ ವಿಶೇಷ ಬಳಕೆದಾರ ಖಾತೆಯನ್ನು ಬಳಸಲು ಸಂಯೋಜನೆ ಮಾಡಲಾಗಿದೆ. ಇದು ಚಟುವಟಿಕೆಗೆ ಅಗತ್ಯವಿರುವ ಕನಿಷ್ಠ ಸವಲತ್ತುಗಳ ತತ್ವವನ್ನು ಉಲ್ಲಂಘಿಸಿತು ಮತ್ತು ಪ್ರಮಾಣತೆಗಳ ಬಹಿರಂಗಪಡಿಕೆಯಿಂದ ಉಂಟಾಗುವ ಅಪಾಯವನ್ನು ಹೆಚ್ಚಿಸಿತು.

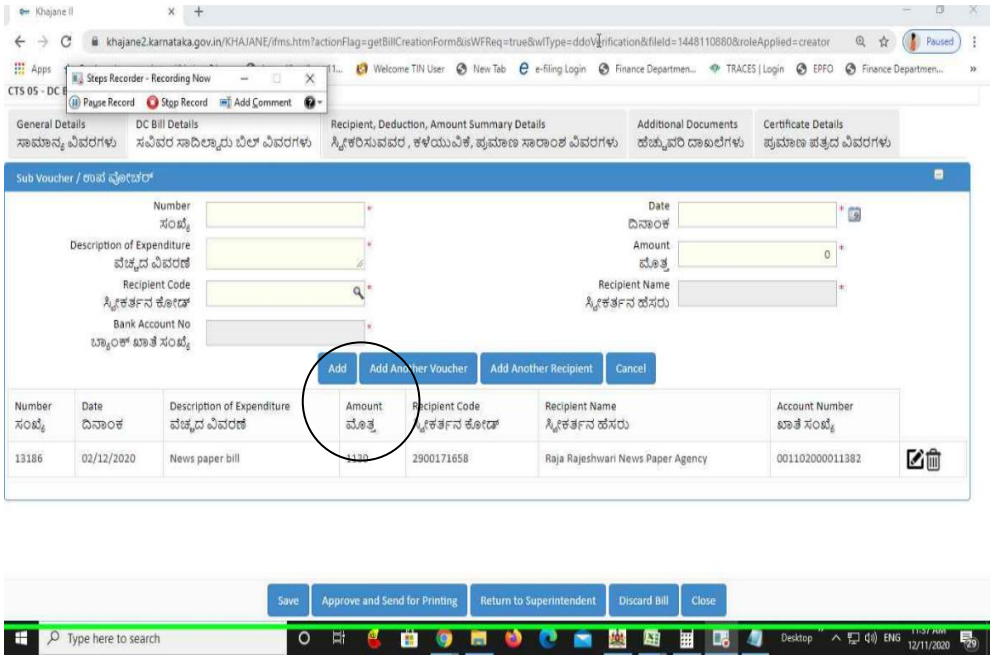
ಇಲಾಖೆಯು ಹಾರ್ಡ್‌ವೇರ್ ಮತ್ತು ಸಾಫ್ಟ್‌ವೇರ್ ಘಟಕಗಳ ಮತ್ತು ಅವುಗಳ ಅಂತರ್–ಸಂಪರ್ಕದ ದಾಸ್ತಾನು ಪಟ್ಟಿಯನ್ನು ಸಿದ್ಧಪಡಿಸುವ ಜೊತೆಗೆ ಅವುಗಳ ದುರ್ಬಲತೆಗಳನ್ನು ದಾಖಲಿಸುವುದರ ಅಗತ್ಯವಿದೆ. ಇಲಾಖೆಯು ಸಾಫ್ಟ್‌ವೇರ್ ಮತ್ತು ಹಾರ್ಡ್‌ವೇರ್ ಘಟಕಗಳನ್ನು ಸಂರಕ್ಷಿಸಲು ಸೂಕ್ತ ಕ್ರಮಗಳನ್ನು ಸಹ ಕೈಗೊಳ್ಳಬೇಕಿದೆ.

4.8.3.2 ಆನ್‌ಲೈನ್ ಸಲ್ಲಿಕೆಯ ನಂತರ ಬಿಲ್ ವಿವರಗಳ ಮಾರ್ಪಾಡು

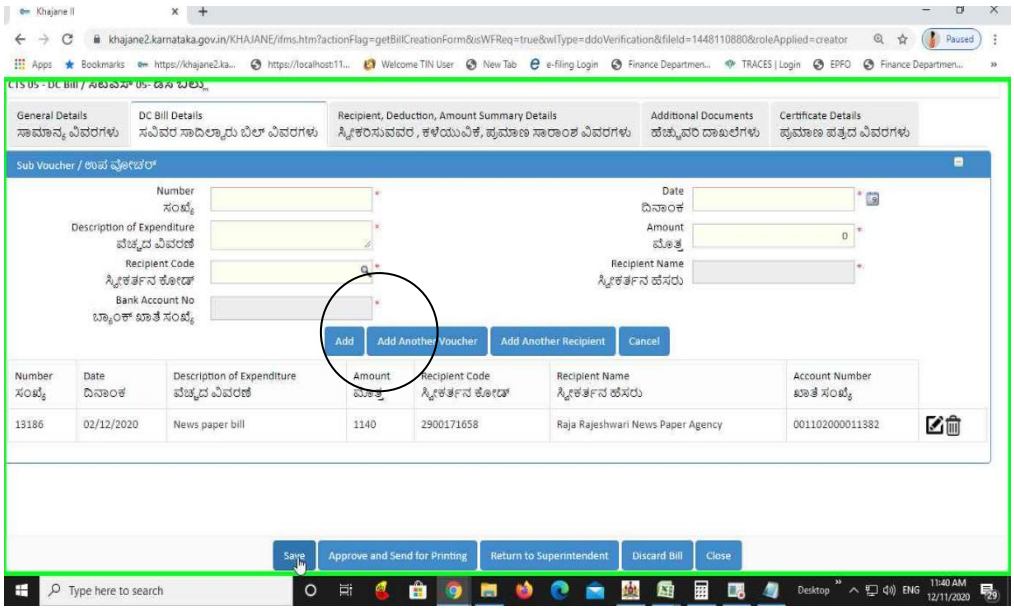
ಕರ್ನಾಟಕ ಮಾಹಿತಿ ಆಯೋಗದ ಕಛೇರಿಯಲ್ಲಿ ಬಿಲ್ ರಚನೆ ಮತ್ತು ಸಲ್ಲಿಕೆ ಕಾರ್ಯಚಟುವಟಿಕೆಯನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ವಿಶ್ಲೇಷಿಸಿತು ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್, ಘಟನೆಗಳ ವೇಳಾಪಟ್ಟಿ ಮತ್ತು ಬಿಲ್‌ಗಳ ಕಾರ್ಯಹರಿವಿನ ಅನುಕ್ರಮವನ್ನು ಆಧರಿಸಿ ಕಾರ್ಯನಿರ್ವಹಣೆ ಪ್ರವೇಶದ ನಿರ್ಬಂಧವನ್ನು ಅನ್ವಯಿಸುವುದಿಲ್ಲ ಎಂಬುದನ್ನು ಗಮನಿಸಿತು. ಇದನ್ನು ಭಿನ್ನ ಪ್ರವೇಶ ನಿಯಂತ್ರಣ ಎಂದು ಕರೆಯಲಾಗುತ್ತದೆ.

ಡಿಡಿಓ ಅವರು ಖಜಾನೆಗೆ ಬಿಲ್ ಅನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಸಲ್ಲಿಸಿದ ನಂತರ ನೌಕರನ ಪಾತ್ರದಿಂದ ಬಿಲ್ ಮೊತ್ತಗಳನ್ನು (ಎರಡು ಬಿಲ್‌ಗಳು) ಮಾರ್ಪಡಿಸುವ ಮೂಲಕ ಭದ್ರತೆಯಲ್ಲಿನ ದೋಷವನ್ನು ಪ್ರದರ್ಶಿಸಲಾಯಿತು (ಡಿಸೆಂಬರ್ 2020). ಖಜಾನೆ ಅಧಿಕಾರಿಗಳು ನೋಡಿದ ಪರದೆಗಳು ಬದಲಾದ ಮೊತ್ತವನ್ನು ತೋರಿಸಿದವು ಮತ್ತು ಇದರಿಂದ ಅಪ್ಲಿಕೇಶನ್ ಬಿಲ್ ಅನ್ನು ಡಿಜಿಟಲ್ ಸಹಿ ಮತ್ತು ಅಧಿಕೃತ ಅಧಿಕಾರಿಯಾದ ಡಿಡಿಓ ಅವರೇ ಸಲ್ಲಿಸಿದ್ದಾರೆ ಎಂದು ಪರಿಗಣಿಸುವುದಿಲ್ಲವಾದರೂ ನೌಕರ ಸಲ್ಲಿಸಿದ ಮೊತ್ತವನ್ನು ಪ್ರಕ್ರಿಯೆಗೊಳಿಸುತ್ತದೆ. ಇದು ಪ್ರಕ್ರಿಯೆಗೊಳಿಸಲಾದ ಮೊತ್ತಗಳ ನಿಖರತೆಯನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಡಿಜಿಟಲ್ ಸಹಿಗಳನ್ನು ಬಳಸಲಾಗುವುದಿಲ್ಲ ಎಂಬುದನ್ನು ತೋರಿಸುತ್ತದೆ.

ಮಾರ್ಪಾಡು ಮಾಡುವ ಮೊದಲಿನ ಬಿಲ್‌ನ ಸ್ಕ್ರೀನ್‌ಶಾಟ್



ಮಾರ್ಪಾಡು ಮಾಡಿದ ನಂತರದ ಬಿಲ್‌ನ ಸ್ಕ್ರೀನ್‌ಶಾಟ್



ಬಿಲ್‌ಗಳನ್ನು ಅಂಗೀಕರಿಸಲು ಮತ್ತು ಅವುಗಳನ್ನು ಖಜಾನೆಗೆ ರವಾನಿಸಲು ಓರ್ವ ನೌಕರನು ಅಧೀಕ್ಷಕರು, ಡಿಡಿಓ ಮತ್ತು ಸಿಎಸ್‌ಓ ಪಾತ್ರವನ್ನು ವಹಿಸಬಹುದಾಗಿದೆಯಾದ್ದರಿಂದ, ವ್ಯವಸ್ಥೆಯು ಕೆಳಗಿನಿಂದ ಮೇಲಿನವರೆಗಿನ ಎಲ್ಲಾ ಹುದ್ದೆಗಳ ವಿಶೇಷಾಧಿಕಾರಗಳನ್ನೂ ಅನುಮತಿಸುತ್ತದೆ ಎಂಬುದನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು. ವ್ಯವಸ್ಥೆಯಲ್ಲಿ ನೌಕರ ಮತ್ತು ಅಧೀಕ್ಷಕರ ಪಾತ್ರಗಳನ್ನು ಮಾತ್ರ ಹೊಂದಿಕೆ ಮಾಡಿದಂತಹ ಓರ್ವ ಬಳಕೆದಾರರ (ಲೆಕ್ಕಾಧೀಕ್ಷಕರು) ಹೆಸರಿನಲ್ಲಿ ಟೋಕನ್ ಸಂಖ್ಯೆ 200556592 ಹೊಂದಿದ ₹1,620 ಮೊತ್ತದ ಬಿಲ್ ಸಂಖ್ಯೆ AD2009116951 ಅನ್ನು ರಚಿಸಲಾಯಿತು (ನೌಕರನ ಪಾತ್ರ), ಪರಿಶೀಲಿಸಲಾಯಿತು (ಅಧೀಕ್ಷಕರ ಪಾತ್ರ) ಮತ್ತು ಅನುಮೋದಿಸಲಾಯಿತು (ಡಿಡಿಓ ಪಾತ್ರ).

ಲೆಕ್ಕಪರಿಶೋಧನೆಗೆ ಒದಗಿಸಲಾದ ಪರೀಕ್ಷಾ ವಿಧಾನಗಳಿಂದ ತಿಳಿದುಬಂದಂತೆ ಪಾವತಿ ಮಾಡಿದ ನಂತರವೂ 62ಬಿ[23] ನಮೂನೆಯನ್ನು ತಿದ್ದಲು ಅನುವು ಮಾಡುವುದರಿಂದ ವ್ಯವಸ್ಥೆಯು ದುರ್ಬಲವಾಗಿದೆ ಎಂದೂ ತೋರಿಸಿತು. ಪ್ರದರ್ಶಿಸಿದ ಮೇಲಿನ ದುರ್ಬಲತೆಗಳು ವ್ಯವಸ್ಥೆಯನ್ನು ಬಿಲ್‌ಗಳು ಮತ್ತು 62ಬಿ ನಮೂನೆಯ ತಿದ್ದುಪಡಿಯ ಅಪಾಯಕ್ಕೆ ಎಡೆಮಾಡುತ್ತವೆ.

ತಾಂತ್ರಿಕ ಸಂಯೋಜಕರು ದುರ್ಬಲತೆಯ ಹೆಚ್ಚಿನ ಪ್ರದರ್ಶನಕ್ಕಾಗಿ ವಿನಂತಿಸಿದರು (ಜೂನ್ 2021). ಅದರಂತೆ ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಖಜಾನೆಗಳ ಆಯುಕ್ತರ ಕಛೇರಿಯಲ್ಲಿಯ ನೌಕರರೊಬ್ಬರ ಸಹಯೋಗದೊಂದಿಗೆ ವೀಡಿಯೊ ಸಭೆಯ ಮೂಲಕ ತಾಂತ್ರಿಕ ಸಂಯೋಜಕರಿಗೆ ಅಪ್ಲಿಕೇಶನ್ ಹೊಂದಿರುವ ಭದ್ರತಾ ದುರ್ಬಲತೆಗಳನ್ನು ಪ್ರದರ್ಶಿಸಿತು (ಜುಲೈ 2021).

ಓರ್ವ ನೌಕರ, ಅಪ್ಲಿಕೇಶನ್‌ನಲ್ಲಿನ ದುರ್ಬಲತೆಯನ್ನು ಹೇಗೆ ಬಳಸಿಕೊಳ್ಳಬಹುದು ಮತ್ತು ಯುಆರ್‌ಎಲ್‌ಗಳನ್ನು ಬದಲಾಯಿಸುವ ಮೂಲಕ ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್‌ಗೆ ಅನಧಿಕೃತ ವಿನಂತಿಗಳನ್ನು ಸಲ್ಲಿಸುವ ಮೂಲಕ ಅಧೀಕ್ಷಕ ಮತ್ತು ಡಿಡಿಓ ಮತ್ತು ಮೇಲುಸಹಿ ಮಾಡುವ ಅಧಿಕಾರಿಯ ಕಾರ್ಯ ನಿರ್ವಹಿಸಬಹುದು ಮತ್ತು ಹೊಸ ಯುಆರ್‌ಎಲ್‌ಗಳನ್ನು ರಚಿಸಲು ಬಳಸಲಾಗುವ ಗುಪ್ತ ದಾಖಲೆಗಳ ಸ್ಥಳವನ್ನು ದುರ್ಬಳಕೆ ಮಾಡಬಹುದಾದ ವಿಧಾನಗಳ ಪ್ರಕ್ರಿಯೆ ಮತ್ತು ಕ್ರಮಗಳನ್ನು ತೋರಿಸಲಾಯಿತು. ಇದಕ್ಕೆ ಅಪ್ಲಿಕೇಶನ್‌ನ ಪ್ರತಿಕ್ರಿಯೆಯನ್ನು ತೋರಿಸಲಾಯಿತು ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್ ಅನಧಿಕೃತವಾಗಿ ಬಿಲ್ ಮೊತ್ತವನ್ನು ಮಾರ್ಪಡಿಸಲು ನೌಕರನಿಗೆ ಅನುಮತಿ ನೀಡುವ ಬಗೆಯನ್ನೂ ಸಹ ಪ್ರದರ್ಶಿಸಲಾಯಿತು. ಈ ಉದ್ದೇಶಕ್ಕಾಗಿ ಒಂದು ಲಕ್ಷ ರೂಪಾಯಿ ಮೊತ್ತಕ್ಕೆ ಹೊಸ ಬಿಲ್ ರಚಿಸಲಾಯಿತು ಮತ್ತು ಮೊತ್ತವನ್ನು ಅನಧಿಕೃತವಾಗಿ ತಿದ್ದುವ ಮೂಲಕ ಎರಡು ಲಕ್ಷ ರೂಪಾಯಿಗಳಿಗೆ ಬದಲಾಯಿಸಲಾಯಿತು.

ಸಮಸ್ಯೆಯನ್ನು ವಿಶ್ಲೇಷಿಸಲಾಗಿದೆ ಮತ್ತು ಪರಿಹರಿಸಲಾಗಿದೆ ಎಂದು ಸರ್ಕಾರವು ಉತ್ತರಿಸಿತು (ನವೆಂಬರ್ 2021). ಆದಾಗ್ಯೂ, ದೋಷವು ಮುಂದುವರಿದಿದೆ ಮತ್ತು ಪ್ರಸ್ತುತ ದಿನಾಂಕದವರೆಗೂ (ನವೆಂಬರ್ 2021) ಬಿಲ್‌ಗಳ ಅನಧಿಕೃತ ತಿದ್ದುಪಡಿ ಸಾಧ್ಯ ಎಂಬುದನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು.

ಇಲಾಖೆಯು ಸರ್ವರ್ ದೃಢೀಕರಣಕ್ಕಾಗಿ ಎಲ್ಲಾ ಸೂಕ್ಷ್ಮ ಬಳಕೆದಾರ ಅಂತರ್–ಸಂಪರ್ಕಸಾಧನ(ಗಳ) ಪರಿಶೀಲನೆಯನ್ನು ಕೈಗೊಳ್ಳಬೇಕು ಮತ್ತು ದೃಢೀಕರಣ ನಿಯಂತ್ರಣಗಳನ್ನು ಅಳವಡಿಸಬೇಕು. ಉತ್ಪಾದನೆಗೆ ಪ್ಯಾಚ್ ಅನ್ನು ಬಿಡುಗಡೆ ಮಾಡುವ ಮೊದಲು ದುರ್ಬಲತೆಗಳ ಪ್ಯಾಚ್‌ಗಳನ್ನು ಸರಿಯಾಗಿ ಪರೀಕ್ಷಿಸಬೇಕು ಮತ್ತು ಅವುಗಳ ಪರಿಣಾಮಕಾರಿತ್ವವನ್ನು ಪರಿಶೀಲಿಸಬೇಕು.

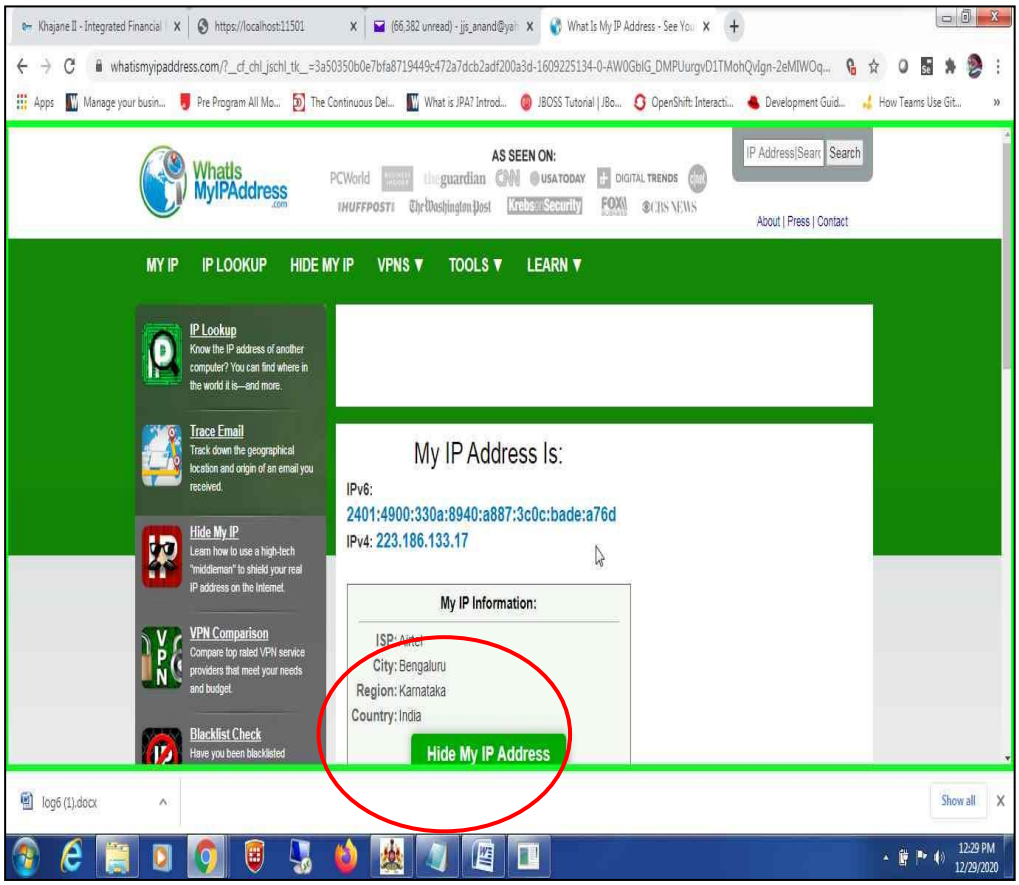
4.8.3.3 ಖಜಾನೆ ಲಾಗಿನ್‌ಗಳ ಮೇಲೆ ಪರಿಣಾಮಕಾರಿಯಲ್ಲದ ನಿರ್ಬಂಧಗಳು

ಬಿಲ್‌ಗಳನ್ನು ಪ್ರಕ್ರಿಯೆಗೊಳಿಸಲು ಖಜಾನೆಗಳಲ್ಲಿ ಕೆಲಸ ಮಾಡುವ ಖಜಾನೆ ಸಿಬ್ಬಂದಿ ಕೆ2ವಿನ ಬಳಕೆದಾರರ ಒಂದು ಗುಂಪಾಗಿ ಗುರುತಿಸಲ್ಪಡುತ್ತಾರೆ. ಈ ಬಳಕೆದಾರರು ಕೆಎಸ್‌ಡಬ್ಲ್ಯುಎಎನ್ ನೆಟ್‌ವರ್ಕ್‌ನಿಂದ ಸಂಪರ್ಕ ಹೊಂದಿದ್ದಾರೆ ಮತ್ತು ಇವರಿಗೆ ಖಜಾನೆ ಹೊರತುಪಡಿಸಿ ಮನೆಯಿಂದ ಅಥವಾ ಬೇರೆಡೆಯಿಂದ ಕೆಲಸ ಮಾಡಲು ಅನುಮತಿ ಇರುವುದಿಲ್ಲ. ಆದಾಗ್ಯೂ, ಖಜಾನೆ ಸಿಬ್ಬಂದಿ ವೈಯಕ್ತಿಕ ಇಂಟರ್ನೆಟ್ ಮೂಲಕ ವೈಯಕ್ತಿಕ ಸಾಧನಗಳನ್ನು ಬಳಸಿಕೊಂಡು ಕೆಲಸ ಮಾಡುವುದನ್ನು ಅಪ್ಲಿಕೇಶನ್ ತಡೆಯುವುದಿಲ್ಲ ಎಂಬುದನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು.

ಖಜಾನೆ ಬಳಕೆದಾರರು ಕೆಎಸ್‌ಡಬ್ಲ್ಯುಎಎನ್ ಹೊರಗಿನಿಂದ ಕೆ2ವಿಗೆ ಲಾಗಿನ್ ಮಾಡಿದಾಗ, ಖಜಾನೆ ಬಳಕೆದಾರರು ಕೆಎಸ್‌ಡಬ್ಲ್ಯುಎಎನ್ ಮೂಲಕ ಲಾಗಿನ್ ಮಾಡಿದಾಗ ಮಾತ್ರ ಇವುಗಳನ್ನು ಒದಗಿಸುವುದರಿಂದ, ವಿವಿಧ ಖಜಾನೆ ಕಾರ್ಯಗಳನ್ನು ಮಾಡಲು ಅಪ್ಲಿಕೇಶನ್ ಮೆನುಗಳನ್ನು ಪೂರೈಸುವುದಿಲ್ಲ ಎಂಬುದನ್ನೂ ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು.

[23] ಕೆಟಿಸಿ 62B ವರದಿಯು ಡಿಡಿಓರವರ ಮಾಸಿಕ ವೆಚ್ಚದ ಲೆಕ್ಕಶೀರ್ಷಿಕೆವಾರು ವಿವರಗಳನ್ನು ಒದಗಿಸುತ್ತದೆ

ಆದಾಗ್ಯೂ, ಬೆಂಗಳೂರಿನ ರಾಜ್ಯ ಹುಜೂರ್ ಖಜಾನೆಯಲ್ಲಿ ಈ ನಿರ್ಬಂಧವನ್ನು ತಪ್ಪಿಸುವ ಮೂಲಕ ವೈಯಕ್ತಿಕ ಮೊಬೈಲ್ ಇಂಟರ್ನೆಟ್ ಸಂಪರ್ಕ ಮತ್ತು ಲ್ಯಾಪ್‌ಟಾಪ್ ಮೂಲಕ ಕೆ2ವಿಗೆ ಲಾಗಿನ್ ಮಾಡುವ ಮತ್ತು ಖಜಾನೆ ಕಾರ್ಯಗಳನ್ನು ನಿರ್ವಹಿಸುವ ಪ್ರಕ್ರಿಯೆಯನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಪ್ರದರ್ಶಿಸಿದ ಕಾರಣ ಈ ನಿರ್ಬಂಧವು ಕೇವಲ ಮೇಲ್ನೋಟಕ್ಕಷ್ಟೇ ಇರುವುದು ಕಂಡುಬಂದಿತು. ವೈಯಕ್ತಿಕ ನೆಟ್‌ವರ್ಕ್ (ಏರ್‌ಟೆಲ್) ಬಳಕೆ ಮತ್ತು ಖಜಾನೆ ವಹಿವಾಟು ನಡೆಸಿದ ಸ್ಕ್ರೀನ್‌ಶಾಟ್ ಅನ್ನು ಕೆಳಗೆ ನೀಡಲಾಗಿದೆ.



4.9 ವಹಿವಾಟು ಮುಂದುವರಿಕೆ ಮತ್ತು ವಿಪತ್ತು ಚೇತರಿಕೆ ಯೋಜನೆಗಳು

ಕೆ2ವಿನಲ್ಲಿ, ವಹಿವಾಟು ಮುಂದುವರಿಕೆ ಮತ್ತು ವಿಪತ್ತು ಚೇತರಿಕೆ ಎರಡೂ ಅಂಶಗಳನ್ನು ವಿಪತ್ತು ಚೇತರಿಕೆ ತಂತ್ರವಾಗಿ ಒಂದೇ ಕಾರ್ಯಚಟುವಟಿಕೆಯಲ್ಲಿ ಸಂಯೋಜಿಸಲಾಗಿದೆ, ಇದು ವಿಪತ್ತಿನ ಸಂದರ್ಭದಲ್ಲಿ ಅಳವಡಿಸಿಕೊಳ್ಳಬೇಕಾದ ವಿಧಾನವನ್ನು ತಿಳಿಸುತ್ತದೆ. ಈ ತಂತ್ರಗಳು/ಯೋಜನೆಗಳನ್ನು ಅವುಗಳ ದಕ್ಷತೆ ಮತ್ತು ಪರಿಣಾಮಕಾರಿತ್ವಕ್ಕಾಗಿ ನಿಯತಕಾಲಿಕವಾಗಿ ಪರೀಕ್ಷಿಸುವುದು ಸಹ ಮುಖ್ಯವಾಗಿದೆ. ಆವರ್ತಕ ಪರೀಕ್ಷೆಯು ವಹಿವಾಟು ಕಾರ್ಯಾಚರಣೆಗಳ ಮತ್ತು ಸೇವೆಗಳ ಮೇಲೆ ಪರಿಣಾಮ ಬೀರುವ ಯೋಜಿತವಲ್ಲದ ಅಡಚಣೆಯ ಸಂದರ್ಭದಲ್ಲಿ ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳ ತ್ವರಿತ ಚೇತರಿಕೆಗೆ ಸಹಕಾರಿಯಾಗಿರುತ್ತದೆ. ಇಲಾಖೆಯ ವಿಪತ್ತಿನ ಪ್ರೊಫೈಲ್ ಮತ್ತು ಅಗತ್ಯತೆಗಳಿಗೆ ಅನುಗುಣವಾಗಿ ಯೋಜನೆಗಳನ್ನು ಅಭಿವೃದ್ಧಿಪಡಿಸಲಾಗಿದೆಯೇ ಮತ್ತು ಪರೀಕ್ಷಿಸಲಾಗಿದೆಯೇ ಎಂದು ಹಿರಿಯ ನಿರ್ವಹಣೆ ತಂಡ ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಬೇಕು

4.9.1 ಯೋಜನೆಗಳ ಪರೀಕ್ಷೆ

ಮಾಸ್ಟರ್ ಸೇವಾ ಒಪ್ಪಂದದ ಪ್ರಕಾರ, ವಹಿವಾಟು ಮುಂದುವರಿಕೆ ತಂತ್ರ/ಯೋಜನೆಯು ಶೂನ್ಯ ದತ್ತಾಂಶ ವಿಳಂಬವನ್ನು ಅನುಸರಿಸಬೇಕು, ಅಂದರೆ, ದತ್ತಸಂಚಯಕ್ಕೆ ರಿಕವರಿ ಪಾಯಿಂಟ್ ಆಬ್ಜೆಕ್ಟಿವ್ (ಆರ್‌ಪಿಒ)[24] ಶೂನ್ಯ ನಿಮಿಷಗಳಾಗಿರಬೇಕು. ವಹಿವಾಟಿನ ನಿರಂತರತೆಯು ಸಂಪೂರ್ಣವಾಗಿ ಕಾರ್ಯನಿರ್ವಹಿಸಲು ಪ್ರಾರಂಭಿಸುವ ಮೊದಲು 10 ರಿಂದ 30 ನಿಮಿಷಗಳ ಕಾಲ ವಿಳಂಬವನ್ನು ಅನುಮತಿಸಲಾಗಿತ್ತು. ಆದಾಗ್ಯೂ, 8 ಡಿಸೆಂಬರ್ 2018 ರಂದು ನಡೆಸಲಾದ ಕೆ2ವಿನ ವಿಪತ್ತು ಚೇತರಿಕೆ ಡ್ರಿಲ್ ಮೇಲಿನ ಪ್ರಕ್ರಿಯೆಗೆ ಸುಮಾರು 188 ನಿಮಿಷಗಳನ್ನು ತೆಗೆದುಕೊಂಡಿತು. ಡ್ರಿಲ್ ಚಟುವಟಿಕೆ ವರದಿ (ಡಿಏಆರ್) ಪ್ರಕಾರ, 'ಡಿಎಸ್‌ಸಿ ಸಹಿ ಮತ್ತು ಬಿಲ್ ರವಾನೆ ಅನುಮೋದನೆ ಮಟ್ಟ'ದಲ್ಲಿನ ಕಾರ್ಯವು ವಿಫಲವಾಗಿತ್ತು. ಸ್ವಿಚ್‌ಓವರ್ ಸಮಯವನ್ನು ಕಡಿಮೆ ಮಾಡಲು, ವರ್ಚುವಲ್ ಯಂತ್ರಗಳ ಸಾಫ್ಟ್‌ವೇರ್ ಸ್ಥಾಪನೆಗೆ, ಅಂತಿಮ ಬಳಕೆದಾರರು ಯಾವುದೇ ಬದಲಾವಣೆ ಮಾಡದಿರಲು ಸಾಕಷ್ಟು ಯುಆರ್‌ಎಲ್ ಮರುನಿರ್ದೇಶನ ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು, ಬಾಹ್ಯ ಏಜೆನ್ಸಿಗಳ ಏಕೀಕರಣ ಇವುಗಳಿಗೆ ಡಿಏಆರ್ ಶಿಫಾರಸು ಮಾಡಿದೆ. ವಿಪತ್ತು ಚೇತರಿಕೆ ವ್ಯವಸ್ಥೆಯ ಸಿದ್ಧತೆ ಮತ್ತು ಪರಿಣಾಮಕಾರಿತ್ವವನ್ನು ಪರಿಶೀಲಿಸಲು 2019–20 ಮತ್ತು 2020–21 ಅವಧಿಯಲ್ಲಿ ತ್ರೈಮಾಸಿಕ ಪರೀಕ್ಷೆಗಳನ್ನು ನಡೆಸಲಾಗಿರಲಿಲ್ಲ. ಇದು ವಿಪತ್ತಿನ ಸಂದರ್ಭದಲ್ಲಿ ಕಾರ್ಯಾಚರಣೆಯನ್ನು ಯಶಸ್ವಿಯಾಗಿ ಪುನರಾರಂಭಿಸುವ ಸಾಮರ್ಥ್ಯದ ಬಗ್ಗೆ ಸರ್ಕಾರಕ್ಕೆ ನೀಡಿದ ಭರವಸೆಯನ್ನು ದುರ್ಬಲಗೊಳಿಸಿತು.

ಪರೀಕ್ಷೆಗಳ ಪರಿಣಾಮಕಾರಿತ್ವವನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಮತ್ತು ಡಿಸಿ ಜಾಲದಿಂದ ಚಾಲನೆಯಲ್ಲಿರುವ ಎಲ್ಲಾ ಕೆ2 ಸೇವೆಗಳನ್ನು ವಿಪತ್ತು ಚೇತರಿಕೆ ಜಾಲದಿಂದ ಚಲಾಯಿಸಬಹುದೆಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಇಲಾಖೆಯು ತ್ರೈಮಾಸಿಕದಲ್ಲಿ ಒಮ್ಮೆ ಡಿಸಿ–ಡಿಆರ್ ಪರೀಕ್ಷೆಯನ್ನು ನಡೆಸಲು ಯೋಜಿಸುತ್ತಿದೆ ಎಂದು ಸರ್ಕಾರವು ಹೇಳಿದೆ (ನವೆಂಬರ್ 2021).

4.9.2 ವಿಪತ್ತು ರಿಕವರಿ ಸ್ಥಳ

ಆರ್‌ಎಫ್‌ಪಿ ಅನುಸಾರ, ದತ್ತಾಂಶ ಸೆಂಟರ್‌ಗಾಗಿ ಒಂದು ಸ್ಥಳ ಮತ್ತು ಡಿಆರ್ ಮತ್ತು ಬಿಸಿಪಿಗಾಗಿ ಮತ್ತೊಂದು ಸ್ಥಳವನ್ನು ಹೊಂದಲು ಇಲಾಖೆಯು ಪ್ರಸ್ತಾಪಿಸಿತ್ತು. ಒಂದೇ ರೀತಿಯ ವಿಪತ್ತುಗಳಿಗೆ ಒಳಪಟ್ಟು ಎರಡೂ ಜಾಲಗಳು ಒಟ್ಟಿಗೇ ಸ್ಥಗಿತಗೊಳ್ಳುವುದನ್ನು ತಪ್ಪಿಸಲು ಜಾಲಗಳು ಸಾಕಷ್ಟು ದೂರದಲ್ಲಿರಬೇಕು ಎಂದು ಅತ್ಯುತ್ತಮ ಅಭ್ಯಾಸಗಳು ಪ್ರತಿಪಾದಿಸುತ್ತವೆ. ಆದಾಗ್ಯೂ, ಈ ಎರಡು ಸ್ಥಳಗಳು ಒಂದೇ ಭೌಗೋಳಿಕ ಸ್ಥಳದಲ್ಲಿ ಒಂದು ಕಿಲೋಮೀಟರ್ ಅಂತರದಲ್ಲಿ ನೆಲೆಗೊಂಡಿವೆ ಎಂಬುದನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು

ಡಿಸಿ ಮತ್ತು ಡಿಆರ್ ಜಾಲಗಳು ಭೌಗೋಳಿಕವಾಗಿ ಬೇರ್ಪಟ್ಟಿರುವುದನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಲು ಬೇರೊಂದು ರಾಜ್ಯದ ದತ್ತಾಂಶ ಸೆಂಟರ್ ಅನ್ನು ದೂರದ ಡಿಆರ್‌ನಂತೆ ಮತ್ತು ಅಸ್ತಿತ್ವದಲ್ಲಿರುವ ಡಿಆರ್ ಸೈಟ್ ಅನ್ನು ಹತ್ತಿರದ ಡಿಆರ್ ಆಗಿ ಬಳಸಲಾಗುವುದು ಎಂದು ಸರ್ಕಾರವು ಭರವಸೆ ನೀಡಿದೆ (ನವೆಂಬರ್ 2021).

ಒಂದೇ ಘಟನೆಯಿಂದ ಡಿಸಿ ಮತ್ತು ಡಿಆರ್ ಪರಿಣಾಮ ಬೀರುವ ಅಪಾಯವನ್ನು ಸರಿದೂಗಿಸಲು ಮತ್ತು ಆವರ್ತಕ ಡಿಆರ್ ಪರೀಕ್ಷೆಗಳನ್ನು ಕೈಗೊಳ್ಳಲು ಉದ್ದೇಶಿತ ಸ್ಥಳದಲ್ಲಿ ದೂರದ ಡಿಆರ್ ಅನುಷ್ಠಾನವನ್ನು ಸರ್ಕಾರವು ತ್ವರಿತಗೊಳಿಸಬೇಕು.

[24] ದತ್ತಾಂಶ ನಷ್ಟವನ್ನು ಸಹಿಸಿಕೊಳ್ಳಬಹುದಾದ ಅವಧಿ, K2 ನಲ್ಲಿ ಇದು '0' ನಿಮಿಷಗಳು

4.10 ಹಳತಾದ ಸ್ವತ್ತುಗಳ ನಿರ್ವಹಣೆ

ಕ್ಷಿಪ್ರವಾಗಿ ಹಳತಾಗುವುದು ಐಟಿ ಸ್ವತ್ತುಗಳ ಗುಣಲಕ್ಷಣಗಳಾಗಿವೆ. ಹಳತಾದ ಸ್ವತ್ತುಗಳ ನಿರ್ವಹಣಾ ಯೋಜನೆಯು ತಂತ್ರಜ್ಞಾನ ಮಾರ್ಗನಕ್ಷೆ, ಘಟಕಗಳ ಸೂಕ್ಷ್ಮತೆಯನ್ನು ಗುರುತಿಸುವುದು, ಎಲ್ಲಾ ಘಟಕಗಳನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡುವುದು ಮುಂತಾದ ವಿವಿಧ ಅಂಶಗಳನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ. ಸೂಕ್ಷ್ಮ ವ್ಯವಸ್ಥೆಗಳಲ್ಲಿ ಹಳತಾದ ಅಥವಾ ಬಳಕೆಯಲ್ಲಿಲ್ಲದ ತಂತ್ರಜ್ಞಾನದ ಬಳಕೆಯನ್ನು ಸಾಧ್ಯವಾದಷ್ಟು ತಪ್ಪಿಸಬೇಕು. ಸ್ಥಾಪನೆಯಿಂದ ಅದರ ಕಾರ್ಯನಿರ್ವಹಣೆಯ ಅಂತ್ಯದವರೆಗೆ ಸಂಗ್ರಹಿಸಲಾದ ವಿವಿಧ ಸ್ವತ್ತುಗಳು ಹಳತಾಗಿರುವುದನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡುವ ಯೋಜನೆಯನ್ನು ಇಲಾಖೆಯು ಹೊಂದಿರಲಿಲ್ಲ.

2019ರ ಅವಧಿಯಲ್ಲಿ ಹಸ್ತಾಂತರಿಸುವ ಭಾಗವಾಗಿ ರಚಿಸಲಾದ ದಸ್ತಾವೇಜನ್ನು ಇಂದೀಕರಿಸಲಾಗಿರಲಿಲ್ಲ ಮತ್ತು ಸಿಸ್ಟಮ್ ವಿನ್ಯಾಸದಲ್ಲಿನ ಬದಲಾವಣೆಗಳನ್ನು ಅಥವಾ ಇತರ ಸಿಸ್ಟಮ್‌ಗಳಿಗೆ (ಆಂತರಿಕ ಮತ್ತು ಬಾಹ್ಯ) ಹೊಸ ಅಂತರ್–ಸಂಪರ್ಕಸಾಧನಗಳನ್ನು ದಾಖಲಿಸಿರಲಿಲ್ಲ ಎಂಬುದನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು. ಸಿಸ್ಟಮ್ ಅಂತರ್–ಸಂಪರ್ಕಸಾಧನಗಳು ಮತ್ತು ಕಾರ್ಯನಿರ್ವಹಣೆಯ ಸ್ಪಷ್ಟ ತಿಳುವಳಿಕೆ ಇಲ್ಲದಿರುವುದು ಬದಲಾವಣೆಗಳು, ಘಟನೆಗಳು ಅಥವಾ ವಿಪತ್ತು ಚೇತರಿಕೆಯ ಘಟನೆಯ ಸಂದರ್ಭದಲ್ಲಿ ಸಿಸ್ಟಮ್ ವೈಫಲ್ಯದ ಅಪಾಯವನ್ನು ಹೆಚ್ಚಿಸುತ್ತದೆ. ಅಂತರ್–ಸಂಪರ್ಕಸಾಧನಗಳಲ್ಲಿನ ದೌರ್ಬಲ್ಯಗಳನ್ನು ಬಳಸಿಕೊಳ್ಳುವ ಮೂಲಕ ಮಾಹಿತಿಗೆ ಸೂಕ್ತವಲ್ಲದ ಪ್ರವೇಶದ ಹೆಚ್ಚುವರಿ ಅಪಾಯವೂ ಇದೆ.

ಹಳತಾದ ಐಟಿ ಸ್ವತ್ತುಗಳನ್ನು ನಿರ್ವಹಿಸಲು ಇಲಾಖೆಯು ಅಪ್ರಚಲಿತತೆ ನೀತಿಯನ್ನು ರಚಿಸುತ್ತದೆ ಎಂದು ಸರ್ಕಾರವು ಭರವಸೆ ನೀಡಿದೆ (ನವೆಂಬರ್ 2021).

4.11 ನಿರ್ಗಮನ ನಿರ್ವಹಣೆ

ಸೇವೆಗಳ ವಿತರಣೆಯ ಸುಗಮ, ನಡೆಯುತ್ತಿರುವ ವಿತರಣೆಗೆ ಕನಿಷ್ಠ ಅಡ್ಡಿ ಮತ್ತು ಅಕಾಲಿಕವಾಗಿ ಮತ್ತು ಯೋಜಿತವಾಗಿ ಗುತ್ತಿಗೆದಾರನ ನಿರ್ಗಮನದ ಸಂದರ್ಭದಲ್ಲಿ ಕಾನೂನು ಕ್ರಮ ಜಾರಿಗೊಳಿಸುವಿಕೆ ಸೇರಿದಂತೆ ಎಲ್ಲಾ ಒಪ್ಪಂದದ ಜವಾಬ್ದಾರಿಗಳನ್ನು ಸಮರ್ಥವಾಗಿ ಪೂರ್ಣಗೊಳಿಸಲು ಪ್ರತಿಯೊಂದು ಯೋಜನೆಯು ಪರಿಣಾಮಕಾರಿ ಸ್ಥಿತ್ಯಂತರಕ್ಕೆ ಅನುಕೂಲವಾಗುವಂತೆ ನಿರ್ಗಮನ ನಿರ್ವಹಣಾ ಯೋಜನೆಯನ್ನು ಹೊಂದಿರಬೇಕು. ಕೆ2ವು ಔಪಚಾರಿಕವಾಗಿ ಯೋಜಿತ, ಅನುಮೋದಿತ ಮತ್ತು ಅಳವಡಿಸಿಕೊಂಡ ನಿರ್ಗಮನ ನಿರ್ವಹಣಾ ಯೋಜನೆಯನ್ನು ಹೊಂದಿರಲಿಲ್ಲ ಎಂಬುದನ್ನು ಲೆಕ್ಕಪರಿಶೋಧನೆಯು ಗಮನಿಸಿತು. ಇದು ಗುತ್ತಿಗೆದಾರರ ಮೇಲೆ ಅವಲಂಬನೆಯನ್ನು ಹೆಚ್ಚಿಸುತ್ತದೆ ಮತ್ತು ಗುತ್ತಿಗೆದಾರರು ನಿರ್ಗಮಿಸುವ ಸಂದರ್ಭದಲ್ಲಿ ವಹಿವಾಟಿನ ನಿರಂತರತೆಯ ಮೇಲೆ ಪರಿಣಾಮ ಬೀರುತ್ತದೆ.

ಇ–ಆಡಳಿತ ಯೋಜನೆಗಳ ಮೇಲಿನ ಕಾರ್ಯತಂತ್ರದ ನಿಯಂತ್ರಣದ ಕುರಿತಾದ ಭಾರತ ಸರ್ಕಾರದ ಮಾರ್ಗಸೂಚಿಗಳು ಇ–ಆಡಳಿತ ಯೋಜನೆಗಳ ಮೇಲೆ ಕಾರ್ಯತಂತ್ರದ ನಿಯಂತ್ರಣವನ್ನು ಸಾಧಿಸುವ ಕ್ರಮಗಳಲ್ಲಿ ನಿರ್ಗಮನ ನಿರ್ವಹಣಾ ಯೋಜನೆಯನ್ನು ಒಂದು ಎಂದು ಪರಿಗಣಿಸುತ್ತವೆ.

ಮಾಸ್ಟರ್ ಸೇವಾ ಒಪ್ಪಂದವು ನಿರ್ಗಮನ ನಿರ್ವಹಣೆಯ ಪ್ರಾಮುಖ್ಯತೆಯನ್ನು ಗುರುತಿಸಿದೆಯಾದರೂ ಮತ್ತು ಅದನ್ನು ಒದಗಿಸಿದೆಯದರೂ, ಇಲಾಖೆಯು ಒಪ್ಪಂದದ ಈ ಭಾಗವನ್ನು ಜಾರಿಗೊಳಿಸಿರಲಿಲ್ಲ. ಹೀಗಾಗಿ, ತಾಂತ್ರಿಕ ಸಂಯೋಜಕರು ನಿರ್ಗಮಿಸುವ ಸಂದರ್ಭ ಉದ್ಭವಿಸಿದಲ್ಲಿ ಕೆ2ವಿನ ಸೇವೆಗಳಿಗೆ ಭಂಗವುಂಟಾಗುವ ಅಪಾಯಕ್ಕೆ ಒಡ್ಡಿದಂತಾಗಿದೆ.

ಕೆ2 ವಿವರವಾದ ನಿರ್ಗಮನ ನಿರ್ವಹಣಾ ಯೋಜನೆಯನ್ನು ಸಿದ್ಧಪಡಿಸುತ್ತದೆ ಎಂದು ಸರ್ಕಾರವು ಭರವಸೆ ನೀಡಿದೆ (ನವೆಂಬರ್ 2021).