

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

1. ಉದ್ದೇಶ

Somindra ಸಂಸ್ಥೆಯು ಮಾಹಿತಿ ಮತ್ತು ಮಾಹಿತಿ-ಸಂಸ್ಕರಣಾ ಆಸ್ತಿಗಳ ಗೌಪ್ಯತೆ, ಸಮಗ್ರತೆ ಮತ್ತು ಲಭ್ಯತೆಯನ್ನು ರಕ್ಷಿಸಲು ಹಾಗೂ ತನ್ನ ಗ್ರಾಹಕರಿಗೆ ವಿಶ್ವಾಸಾರ್ಹ, ಸುರಕ್ಷಿತ ಮತ್ತು ಪರಿಣಾಮಕಾರಿ IT ಆಧಾರಿತ ಸೇವೆಗಳನ್ನು ಒದಗಿಸಲು ಬದ್ಧವಾಗಿದೆ.

ಈ ಸಮಗ್ರ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು IT ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿಯು ಸಂಸ್ಥೆಯ ಕೆಳಗಿನ ವಿಷಯಗಳತ್ತ ಒಟ್ಟಾರೆ ದಿಕ್ಕು ಮತ್ತು ಬದ್ಧತೆಯನ್ನು ನಿರ್ಧರಿಸುತ್ತದೆ:

- ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಸೈಬರ್ ಭದ್ರತೆ;
- ಗ್ರಾಹಕ, ಉದ್ಯೋಗಿ, ಪೂರೈಕೆದಾರ ಮತ್ತು ವ್ಯವಹಾರ ಮಾಹಿತಿಯ ರಕ್ಷಣೆ;
- IT ಆಧಾರಿತ ಸೇವೆಗಳ ಪರಿಣಾಮಕಾರಿ ನಿರ್ವಹಣೆ;
- ಅನ್ವಯವಾಗುವ ಕಾನೂನು, ನಿಯಂತ್ರಣಾತ್ಮಕ ಮತ್ತು ಒಪ್ಪಂದಾತ್ಮಕ ಅವಶ್ಯಕತೆಗಳ ಪಾಲನೆ;
- ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು IT ಸೇವಾ ಅಪಾಯಗಳ ನಿರ್ವಹಣೆ;
- ಮಾಹಿತಿ ಭದ್ರತಾ ನಿರ್ವಹಣಾ ವ್ಯವಸ್ಥೆ (ISMS) ಮತ್ತು IT ಸೇವಾ ನಿರ್ವಹಣಾ ವ್ಯವಸ್ಥೆ (ITSM) ಯ ನಿರಂತರ ಸುಧಾರಣೆ.

2. ವ್ಯಾಪ್ತಿ

This ನೀತಿ applies to all ಉದ್ಯೋಗಿಗಳು, ನಿರ್ವಹಣೆ, ಒಪ್ಪಂದಾತ್ಮಕ ಸಿಬ್ಬಂದಿ, temporary ಸಿಬ್ಬಂದಿ, ತೃತೀಯ ಪಕ್ಷಗಳು and other interested parties working for or on behalf of Somindra, and to ಮಾಹಿತಿ, technology, facilities and ಸೇವೆಗಳು within the approved certification scope.

ನಿರ್ವಹಣಾ ವ್ಯವಸ್ಥೆಯ ವ್ಯಾಪ್ತಿಯು ಕೆಳಗಿನವುಗಳನ್ನು ಒಳಗೊಂಡಿದೆ:

“Storage, Supply, Installation, Commissioning, Technical Support and Solutions of IT, Networking, Audio/Video Solutions, Power & Energy Solutions, Imaging & Printing, Security Solutions; Storage, Supply & Installation of Telecommunication, Consumer

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)



SOMINDRA MARKETING

ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ
ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ

FORMAT. No :SM/ISIT/POL/01

V.2.0, R.0.0

EFF DATE :21.08.2026

Durables, Smart School Solution Software and Applications, Electronics and Electricals Consumables & Accessories, Automation Solution, Tools & Machinery.”

The ನೀತಿ applies to ಮಾಹಿತಿ handled through ಭೌತಿಕ and electronic means, including organizational computers/laptops, ನೆಟ್ವರ್ಕ್ ಉಪಕರಣಗಳು, email, ಕ್ಲೌಡ್ ಸಂಗ್ರಹಣೆ, business ಅಪ್ಲಿಕೇಶನ್‌ಗಳು, CCTV/NVR ವ್ಯವಸ್ಥೆಗಳು, ಗ್ರಾಹಕರ ಮಾಹಿತಿ, project ಮಾಹಿತಿ and related records.

3. ನಿರ್ವಹಣಾ ಬದ್ಧತೆ

Top Management is committed to establishing, implementing, maintaining and continually improving the ISMS and ITSM ವ್ಯವಸ್ಥೆ in accordance with ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018.

ನಿರ್ವಹಣೆಯು provide ಸೂಕ್ತ ಸಂಪನ್ಮೂಲಗಳು, ಜವಾಬ್ದಾರಿಗಳು, infrastructure, competence and support required for effective operation of these ವ್ಯವಸ್ಥೆಗಳು.

ನಿರ್ವಹಣೆಯು ensure that ಮಾಹಿತಿ ಭದ್ರತೆ and IT ಸೇವಾ ಅವಶ್ಯಕತೆಗಳು are considered in business decisions, ಗ್ರಾಹಕ projects, ಖರೀದಿ, ಸ್ಥಾಪನೆ, ಕಮಿಷನಿಂಗ್, technical support and other ಸಂಬಂಧಿತ activities.

4. ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಸೈಬರ್ ಭದ್ರತಾ ಬದ್ಧತೆ

Somindra ಸಂಸ್ಥೆಯು ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಬಹಿರಂಗಪಡಿಸುವಿಕೆ, ಬದಲಾವಣೆ, ನಷ್ಟ, ದುರುಪಯೋಗ ಮತ್ತು ನಾಶದಿಂದ ಮಾಹಿತಿಯನ್ನು ರಕ್ಷಿಸಬೇಕು.

ಸಂಸ್ಥೆಯು adopt a ಅಪಾಯ-based approach to identify, assess and treat ಮಾಹಿತಿ ಭದ್ರತಾ ಅಪಾಯಗಳು arising from:

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)



SOMINDRA MARKETING

ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ
ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ

FORMAT. No :SM/ISIT/POL/01

V.2.0, R.0.0

EFF DATE :21.08.2026

- ಉದ್ಯೋಗಿಗಳು ಮತ್ತು ತೃತೀಯ ಪಕ್ಷಗಳು;
- IT ಆಸ್ತಿಗಳು ಮತ್ತು ಎಂಡ್‌ಪಾಯಿಂಟ್‌ಗಳು;
- ಇ-ಮೇಲ್ ಮತ್ತು ಕ್ಲೌಡ್ ಸೇವೆಗಳು;
- ನೆಟ್ವರ್ಕ್ ಮೂಲಸೌಕರ್ಯ;
- ಗ್ರಾಹಕ ಮತ್ತು ಯೋಜನಾ ಮಾಹಿತಿ;
- ಸೈಬರ್ ಭದ್ರತಾ ಬೆದರಿಕೆಗಳು;
- ಭೌತಿಕ ಮತ್ತು ಪರಿಸರ ಪರಿಸ್ಥಿತಿಗಳು;
- ಪೂರೈಕೆದಾರರು ಮತ್ತು ತೃತೀಯ ಪಕ್ಷದ ಸೇವೆಗಳು; ಮತ್ತು
- ವ್ಯವಹಾರ ಮತ್ತು ಸೇವಾ ವ್ಯತ್ಯಯಗಳು.

Appropriate administrative, technical and ಭೌತಿಕ controls ಸ್ಥಾಪಿಸಬೇಕು based on identified ಅಪಾಯಗಳು and ಅನ್ವಯವಾಗುವ ಅವಶ್ಯಕತೆಗಳು.

5. IT ಸೇವಾ ನಿರ್ವಹಣಾ ಬದ್ಧತೆ

Somindra ಸಂಸ್ಥೆಯು ಬದ್ಧವಾಗಿದೆ delivering IT-enabled products, solutions and ಸೇವೆಗಳು in a controlled, consistent and ಗ್ರಾಹಕ-focಬಳಸಿದ manner.

ಸಂಸ್ಥೆಯು establish ಸೂಕ್ತ arrangements for:

- ಗ್ರಾಹಕ ಮತ್ತು ಸೇವಾ ಅವಶ್ಯಕತೆಗಳನ್ನು ಅರ್ಥಮಾಡಿಕೊಳ್ಳುವುದು;
- ಸೇವೆಗಳ ಯೋಜನೆ ಮತ್ತು ವಿತರಣೆ;
- ಸ್ಥಾಪನೆ, ಕಾನ್ಪಿಗರೇಶನ್ ಮತ್ತು ಕಮಿಷನಿಂಗ್;

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)



SOMINDRA MARKETING

ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ
ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ

FORMAT. No :SM/ISIT/POL/01

V.2.0, R.0.0

EFF DATE :21.08.2026

- ಸೇವಾ ವಿನಂತಿಗಳು ಮತ್ತು ಘಟನೆಗಳು;
- ಸೇವಾ ಲಭ್ಯತೆ ಮತ್ತು ನಿರಂತರತೆ;
- ಬದಲಾವಣೆ ಮತ್ತು ಕಾನ್ಫಿಗರೇಶನ್ ನಿರ್ವಹಣೆ;
- ಪೂರೈಕೆದಾರ ಮತ್ತು ತೃತೀಯ ಪಕ್ಷದ ನಿರ್ವಹಣೆ;
- ಸೇವಾ ಕಾರ್ಯಕ್ಷಮತೆಯ ಮೇಲ್ವಿಚಾರಣೆ;
- ಗ್ರಾಹಕರ ಪ್ರತಿಕ್ರಿಯೆ ಮತ್ತು ತೃಪ್ತಿ; ಮತ್ತು
- ಸೇವೆಗಳ ನಿರಂತರ ಸುಧಾರಣೆ.

ನಿರ್ದರಿಸಲಾದ ಅವಶ್ಯಕತೆಗಳು, ಉದ್ದೇಶಗಳು ಮತ್ತು ಅನ್ವಯವಾಗುವ ಸೇವಾ-ಮಟ್ಟದ ಬದ್ಧತೆಗಳಿಗೆ ಅನುಗುಣವಾಗಿ ಸೇವಾ ಕಾರ್ಯಕ್ಷಮತೆಯನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಬೇಕು.

6. ಮಾಹಿತಿ ಮತ್ತು ದತ್ತಾಂಶ ರಕ್ಷಣೆ

Somindra ಸಂಸ್ಥೆಯು ensure that ಮಾಹಿತಿ is ಸೂಕ್ತly classified, handled, ಸಂಗ್ರಹಿಸಿದ, ವರ್ಗಾಯಿಸಿದ, retained and disposed of according to its sensitivity and ವ್ಯವಹಾರ ಅವಶ್ಯಕತೆಗಳು.

ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಮತ್ತು ಇತರ ಗೌಪ್ಯ ಮಾಹಿತಿಯನ್ನು ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಬಳಕೆ ಅಥವಾ ಬಹಿರಂಗಪಡಿಸುವಿಕೆಯಿಂದ ರಕ್ಷಿಸಬೇಕು.

Employees and ಸಂಬಂಧಿತ ತೃತೀಯ ಪಕ್ಷಗಳು ಬೇಕು maintain ಗೌಪ್ಯತೆ of ಮಾಹಿತಿ obtained during their association with Somindra.

7. ಜನರು, ಜಾಗೃತಿ ಮತ್ತು ಜವಾಬ್ದಾರಿ

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ಎಲ್ಲಾ ಸಿಬ್ಬಂದಿಯು ತಮ್ಮ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು IT ಸೇವಾ ಜವಾಬ್ದಾರಿಗಳನ್ನು ಅರ್ಥಮಾಡಿಕೊಂಡು ಅನ್ವಯವಾಗುವ ನೀತಿಗಳು, ಕಾರ್ಯವಿಧಾನಗಳು ಮತ್ತು ಸೂಚನೆಗಳನ್ನು ಪಾಲಿಸಬೇಕು.

Somindra ಸಂಸ್ಥೆಯು provide ಸೂಕ್ತ induction, ಜಾಗೃತಿ and ತರಬೇತಿ relating to ಮಾಹಿತಿ ಭದ್ರತೆ, ಸೈಬರ್ ಭದ್ರತೆ, IT ಸೇವಾ ನಿರ್ವಹಣೆ, acceptable ಬಳಕೆ, ಘಟನೆ ವರದಿing, remote working and other ಸಂಬಂಧಿತ ಅವಶ್ಯಕತೆಗಳು.

Roles and ಜವಾಬ್ದಾರಿಗಳು ನಿರ್ಧರಿಸಬೇಕು and communicated to ensure accountability for the operation and ಸುಧಾರಣೆ of the ISMS and ITSM ವ್ಯವಸ್ಥೆ.

8. ಘಟನೆಗಳು, ವಿಪತ್ತುಗಳು ಮತ್ತು ವ್ಯವಹಾರ ನಿರಂತರತೆ

ಮಾಹಿತಿ ಭದ್ರತಾ ಘಟನೆಗಳು ಮತ್ತು IT ಸೇವಾ ಘಟನೆಗಳ ವರದಿ, ಮೌಲ್ಯಮಾಪನ, ಪ್ರತಿಕ್ರಿಯೆ ಮತ್ತು ಅವುಗಳಿಂದ ಕಲಿಯಲು Somindra ಸೂಕ್ತ ವ್ಯವಸ್ಥೆಗಳನ್ನು ಸ್ಥಾಪಿಸಬೇಕು.

ಸಂಸ್ಥೆಯು maintain ಸೂಕ್ತ ಬ್ಯಾಕಪ್, ವಿಪತ್ತು ಮರುಪಡೆಯುವಿಕೆ and ವ್ಯವಹಾರ ನಿರಂತರತೆ arrangements based on business and ಸೇವೆ ಅಪಾಯಗಳು.

Information and critical IT ಆಧಾರಿತ ಸೇವೆಗಳು ರಕ್ಷಿಸಬೇಕು, reಸಂಗ್ರಹಿಸಿದ and recovered within defined and practical ಅವಶ್ಯಕತೆಗಳು following disruption.

9. ಕಾನೂನು, ನಿಯಂತ್ರಣಾತ್ಮಕ ಮತ್ತು ಒಪ್ಪಂದಾತ್ಮಕ ಅನುಸರಣೆ

Somindra ಸಂಸ್ಥೆಯು identify and comply with ಅನ್ವಯವಾಗುವ:

- Legal and statutory ಅವಶ್ಯಕತೆಗಳು;
- Regulatory ಅವಶ್ಯಕತೆಗಳು;

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

- Customer ಅವಶ್ಯಕತೆಗಳು;
- Contractual obligations;
- Confidentiality obligations;
- Intellectual property ಅವಶ್ಯಕತೆಗಳು; and
- Privacy and ದತ್ತಾಂಶ-ರಕ್ಷಣೆ ಅವಶ್ಯಕತೆಗಳು.

ಅನುಸರಣೆಯನ್ನು ಕಾಲಕಾಲಕ್ಕೆ ಪರಿಶೀಲಿಸಿ, ಗುರುತಿಸಲಾದ ಕೊರತೆಗಳಿಗೆ ಸೂಕ್ತ ಕ್ರಮಗಳನ್ನು ಕೈಗೊಳ್ಳಬೇಕು.

10. ಪೂರೈಕೆದಾರರು ಮತ್ತು ತೃತೀಯ ಪಕ್ಷಗಳು

Information-ಭದ್ರತೆ and IT ಸೇವಾ ಅವಶ್ಯಕತೆಗಳು ಪರಿಗಣಿಸಬೇಕು while selecting, engaging and monitoring ಪೂರೈಕೆದಾರರು, ಕ್ಲೌಡ್-ಸೇವೆ providers, OEMs, contractors and other ಸಂಬಂಧಿತ ತೃತೀಯ ಪಕ್ಷಗಳು.

Where ಅನ್ವಯವಾಗುವ, ಗೌಪ್ಯತೆ, ಭದ್ರತೆ, ಸೇವೆ quality, ಲಭ್ಯತೆ, ಘಟನೆ ವರದಿing and ಒಪ್ಪಂದಾತ್ಮಕ ಅವಶ್ಯಕತೆಗಳು ಬೇಕು incorporated into ಪೂರೈಕೆದಾರ arrangements.

11. ಉದ್ದೇಶಗಳು, ಕಾರ್ಯಕ್ಷಮತೆ ಮತ್ತು ನಿರಂತರ ಸುಧಾರಣೆ

Somindra ಸಂಸ್ಥೆಯು establish measurable ಮಾಹಿತಿ ಭದ್ರತಾ and IT ಸೇವೆ objectives ಸೂಕ್ತ to its business, ಅಪಾಯಗಳು and ಗ್ರಾಹಕರ ಅವಶ್ಯಕತೆಗಳು.

Performance ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಬೇಕು through ಸೂಕ್ತ indicators, ಆಡಿಟ್‌ಗಳು, ಪರಿಶೀಲನೆಗಳು, ಘಟನೆಗಳು, ಗ್ರಾಹಕ ಪ್ರತಿಕ್ರಿಯೆ, ಸೇವೆ ಕಾರ್ಯಕ್ಷಮತೆ and ನಿರ್ವಹಣೆ ಪರಿಶೀಲನೆ.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01 V.2.0, R.0.0 EFF DATE :21.08.2026
--	---	---

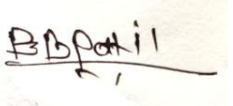
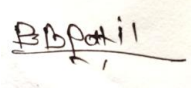
Nonconformities and identified ಸುಧಾರಣೆ opportunities ಪರಿಹರಿಸಬೇಕು through ಸೂಕ್ತ ಸರಿಪಡಿಸುವ ಕ್ರಮ. Somindra ಸಂಸ್ಥೆಯು ಬದ್ಧವಾಗಿದೆ continually improving the suitability, adequacy and effectiveness of its ISMS and ITSM ವ್ಯವಸ್ಥೆ.

12. ನೀತಿ ಪರಿಶೀಲನೆ ಮತ್ತು ಅನುಮೋದನೆ

This ನೀತಿ ಪರಿಶೀಲಿಸಬೇಕು periodically and whenever significant ಬದಲಾವಣೆಗಳು occur in the organization's business, technology, ಸೇವೆಗಳು, ಅಪಾಯಗಳು, ಕಾನೂನು ಅವಶ್ಯಕತೆಗಳು or interested-party ಅವಶ್ಯಕತೆಗಳು.

The ನೀತಿ ತಿಳಿಸಬೇಕು to ಸಂಬಂಧಿತ ಸಿಬ್ಬಂದಿ and made available to ಅನ್ವಯವಾಗುವ interested parties as ಸೂಕ್ತ.

All ಸಿಬ್ಬಂದಿ working for or on behalf of Somindra are expected to comply with this ನೀತಿ and its ಅನ್ವಯವಾಗುವ annexures.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್	ಪರಿಶೀಲಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ ಮತ್ತು ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ	ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ
ಹುದ್ದೆ: CISO	ಹುದ್ದೆ: CISO & MD	ಹುದ್ದೆ: MD
ದಿನಾಂಕ: 01.08.2026	ದಿನಾಂಕ: 01.08.2026	ದಿನಾಂಕ: 01.08.2026
ಸಹಿ: 	ಸಹಿ:  	ಸಹಿ: 

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ಅನುಬಂಧ 01

ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಸೈಬರ್ ಭದ್ರತಾ ನಿಯಮಗಳು

ಉಲ್ಲೇಖ: FTS/ISIT/POL/01 – ಅನುಬಂಧ 01

Somindra ಸಂಸ್ಥೆಯು ರಕ್ಷಿಸು ಮಾಹಿತಿ and ಮಾಹಿತಿ-processing assets against ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಬಹಿರಂಗಪಡಿಸುವಿಕೆ, alteration, ನಷ್ಟ, ದುರುಪಯೋಗ and destruction.

ಮುಖ್ಯ ನಿಯಮಗಳು

1. Information ಮಾತ್ರ ಇರಬೇಕು ಪ್ರವೇಶದ by ಅಧಿಕೃತ ಸಿಬ್ಬಂದಿ having a legitimate business requirement.
2. Confidential/ಗ್ರಾಹಕರ ಮಾಹಿತಿ ಬಾರದು ಬಹಿರಂಗಪಡಿಸಿದ to unauthorized persons.
3. Company ಮಾಹಿತಿ ಬೇಕು ಸಂಗ್ರಹಿಸಿದ only on approved ವ್ಯವಸ್ಥೆಗಳು, ಅಪ್ಲಿಕೇಶನ್‌ಗಳು and ಸಂಗ್ರಹಣೆ locations.
4. Employees ಬಾರದು knowingly introduce malware, unauthorized ಸಾಫ್ಟ್‌ವೇರ್ or other malicious content into company ವ್ಯವಸ್ಥೆಗಳು.
5. Suspicious emails, phishing attempts, malware, ಅನಧಿಕೃತ ಪ್ರವೇಶ, lost ಸಾಧನಗಳು or suspected ಮಾಹಿತಿ leakage ತಕ್ಷಣ ವರದಿ ಮಾಡಬೇಕು.
6. Security updates and controls implemented by Somindra ಸಂಸ್ಥೆಯು not be deliberately disabled or bypassed.
7. Passwords and ದೃಢೀಕರಣ ಮಾಹಿತಿ ಬೇಕು remain confidential.
8. Customer ಮಾಹಿತಿ and ತಾಂತ್ರಿಕ ಮಾಹಿತಿ ಬೇಕು handled only for authorized ವ್ಯವಹಾರ ಉದ್ದೇಶಗಳು.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

9. Information-ಭದ್ರತೆ ಅವಶ್ಯಕತೆಗಳು ಪರಿಗಣಿಸಬೇಕು during ಖರೀದಿ, ಸ್ಥಾಪನೆ, ಕಾನ್ಫಿಗರೇಶನ್ and ಕಮಿಷನಿಂಗ್ of technology solutions.
10. Personnel ಬೇಕು cooperate with ಭದ್ರತೆ investigations, ಆಡಿಟ್‌ಗಳು and ಸರಿಪಡಿಸುವ ಕ್ರಮ.

ಅನುಬಂಧ 02

IT ಮತ್ತು ಮಾಹಿತಿ ಆಸ್ತಿಗಳ ಸ್ವೀಕಾರಾರ್ಹ ಬಳಕೆ

ಉಲ್ಲೇಖ: FTS/ISIT/POL/01 – ಅನುಬಂಧ 02

Company IT assets and ಮಾಹಿತಿ resources ಬಳಸಬೇಕು responsibly, securely and primarily for authorized ವ್ಯವಹಾರ ಉದ್ದೇಶಗಳು.

ಮುಖ್ಯ ನಿಯಮಗಳು

- Company computers, laptops, email, Google Drive, Tally and other IT resources ಬಳಸಬೇಕು only for legitimate purposes.
- Unಅಧಿಕೃತ ಪ್ರವೇಶ to ವ್ಯವಸ್ಥೆಗಳು, accounts, files or ನೆಟ್ವರ್ಕ್‌s ನಿಷೇಧಿಸಲಾಗಿದೆ.
- Users ಬಾರದು share ಪಾಸ್‌ವರ್ಡ್‌ಗಳು or ದೃಢೀಕರಣ credentials.
- Unauthorized ಸಾಫ್ಟ್‌ವೇರ್, ಅಪ್ಲಿಕೇಶನ್‌ಗಳು, extensions or ಸಂಗ್ರಹಣೆ ಸಾಧನಗಳು ಬಾರದು installed or connected.
- Company ಸಾಧನಗಳು ಬಾರದು ಬಳಸಿದ for activities that may create ಭದ್ರತೆ, ಕಾನೂನು or reputational ಅಪಾಯಗಳು.
- Employees ಬೇಕು exercise caution while opening email attachments, links or downloading files.
- Confidential ಮಾಹಿತಿ ಬಾರದು copied to unauthorized personal ಸಂಗ್ರಹಣೆ or shared through unauthorized channels.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

- Users ಬೇಕು lock their computers/screens when unattended.
- Internet resources ಬಳಸಬೇಕು responsibly and in accordance with organizational ಅವಶ್ಯಕತೆಗಳು.
- Any suspected ದುರುಪಯೋಗ, ನಷ್ಟ or compromise of an IT asset ತಕ್ಷಣ ವರದಿ ಮಾಡಬೇಕು.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)
ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ಅನುಬಂಧ 03

ಪ್ರವೇಶ ನಿಯಂತ್ರಣ ಮತ್ತು ದೃಢೀಕರಣ ನಿಯಮಗಳು

ಉಲ್ಲೇಖ: FTS/ISIT/POL/01 – ಅನುಬಂಧ 03

Access to ಮಾಹಿತಿ ಮತ್ತು ವ್ಯವಸ್ಥೆಗಳು ಬೇಕು granted according to business need, role and ಅನುಮೋದನೆ.

ಮುಖ್ಯ ನಿಯಮಗಳು

1. Each ಬಳಕೆ ಬೇಕು ಬಳಕೆ an individually assigned account wherever technically feasible.
2. Passwords ಬೇಕು strong, confidential and ಬಾರದು shared.
3. Multi-factor ದೃಢೀಕರಣ ಬೇಕು enabled where supported and ಸೂಕ್ತ.
4. Access ಬೇಕು granted only after ಸೂಕ್ತ ಅನುಮೋದನೆ.
5. Privileged/administrative ಪ್ರವೇಶ ಬೇಕು restricted to ಅಧಿಕೃತ ಸಿಬ್ಬಂದಿ.
6. Access rights ಪರಿಶೀಲಿಸಬೇಕು periodically and whenever an employee ಬದಲಾವಣೆಗಳು role.
7. Access ಬೇಕು promptly modified or withdrawn when employment or ಜವಾಬ್ದಾರಿಗಳು ಬದಲಾವಣೆ.
8. Users ಬಾರದು attempt to bypass ಪ್ರವೇಶ restrictions.
9. Default ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಬದಲಾಯಿಸಬೇಕು where technically ಅನ್ವಯವಾಗುವ.
10. Authentication ಮಾಹಿತಿ ಬಾರದು ಸಂಗ್ರಹಿಸಿದ or communicated insecurely.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ಅನುಬಂಧ 04

ಮಾಹಿತಿ ವರ್ಗೀಕರಣ, ಗೌಪ್ಯತೆ ಮತ್ತು ದತ್ತಾಂಶ ರಕ್ಷಣಾ ನಿಯಮಗಳು

ಉಲ್ಲೇಖ: FTS/ISIT/POL/01 – ಅನುಬಂಧ 04

Somindra ಸಂಸ್ಥೆಯು ರಕ್ಷಿಸು ಮಾಹಿತಿ according to its sensitivity, business value, ಒಪ್ಪಂದಾತ್ಮಕ obligations and privacy ಅವಶ್ಯಕತೆಗಳು.

ಮಾಹಿತಿ ವರ್ಗಗಳು

ಸಾರ್ವಜನಿಕ: ಸಾರ್ವಜನಿಕವಾಗಿ ಬಹಿರಂಗಪಡಿಸಲು ಅನುಮೋದಿಸಲಾದ ಮಾಹಿತಿ.

ಆಂತರಿಕ: ಅಧಿಕೃತ ಸಂಸ್ಥೆಯ ಬಳಕೆಗಾಗಿ ಉದ್ದೇಶಿಸಲಾದ ಸಾಮಾನ್ಯ ವ್ಯವಹಾರ ಮಾಹಿತಿ.

ಗೌಪ್ಯ: ಗ್ರಾಹಕ, ಪೂರೈಕೆದಾರ, ವಾಣಿಜ್ಯ, ತಾಂತ್ರಿಕ, ಹಣಕಾಸು, ಒಪ್ಪಂದಾತ್ಮಕ ಅಥವಾ ಇತರ ಸಂವೇದನಾಶೀಲ ಮಾಹಿತಿ.

ನಿರ್ಬಂಧಿತ: ಹೆಚ್ಚುವರಿ ಪ್ರವೇಶ ನಿರ್ಬಂಧಗಳ ಅಗತ್ಯವಿರುವ ಅತ್ಯಂತ ಸಂವೇದನಾಶೀಲ ಮಾಹಿತಿ.

ಮುಖ್ಯ ನಿಯಮಗಳು

- Information ಬೇಕು ಪ್ರವೇಶಿತ only for authorized purposes.
- Personal ಮಾಹಿತಿ ಬೇಕು collected, ಬಳಸಿದ, ಸಂಗ್ರಹಿಸಿದ and shared only for legitimate ವ್ಯವಹಾರ ಉದ್ದೇಶಗಳು.
- Confidential ಮಾಹಿತಿ ಬಾರದು ಬಹಿರಂಗಪಡಿಸಿದ without ಅನುಮೋದನೆ.
- Information ಬೇಕು ವರ್ಗಾಯಿಸಿದ through approved and reasonably secure channels.
- Information ಬೇಕು retained only for the required period.
- Unnecessary copies ತಪ್ಪಿಸಬೇಕು.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

- Information ಬೇಕು securely disposed of when no longer required.
- Employees ಬೇಕು maintain ಗೌಪ್ಯತೆ during and after employment.

ಅನುಬಂಧ 05

ದೂರಸ್ಥ ಕೆಲಸ ಮತ್ತು BYOD ನಿಯಮಗಳು

ಉಲ್ಲೇಖ: FTS/ISIT/POL/01 – ಅನುಬಂಧ 05

Somindra permits remote working where authorized and ಬೇಕು apply ಸೂಕ್ತ safeguards to ರಕ್ಷಿಸು organizational and ಗ್ರಾಹಕರ ಮಾಹಿತಿ.

ದೂರಸ್ಥ ಕೆಲಸದ ನಿಯಮಗಳು

- Employees ಬೇಕು work from reasonably secure locations.
- Company laptops/ಸಾಧನಗಳು ರಕ್ಷಿಸಬೇಕು against ಅನಧಿಕೃತ ಪ್ರವೇಶ, theft and ದುರುಪಯೋಗ.
- Screens ಬೇಕು locked when unattended.
- Confidential ಮಾಹಿತಿ ಬಾರದು exposed to unauthorized persons in remote locations.
- Employees ಬೇಕು ಬಳಕೆ approved accounts and ಅಪ್ಲಿಕೇಶನ್‌ಗಳು for business work.
- Public or unsecured ನೆಟ್ವರ್ಕ್‌s ತಪ್ಪಿಸಬೇಕು where reasonably possible.
- Lost or stolen ಸಾಧನಗಳು ತಕ್ಷಣ ವರದಿ ಮಾಡಬೇಕು.

BYOD ನಿಯಮಗಳು

Personal ಸಾಧನಗಳು ಬಾರದು ಬಳಸಿದ for storing or processing confidential/ಗ್ರಾಹಕರ ಮಾಹಿತಿ unless specifically authorized.

Where BYOD is permitted:

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

- The ಸಾಧನ ಬೇಕು have ಸೂಕ್ತ ಭದ್ರತೆ ರಕ್ಷಣೆ.
- Access ಸೀಮಿತಗೊಳಿಸಬೇಕು to authorized business resources.
- Company ಮಾಹಿತಿ ಬಾರದು unnecessarily downloaded or retained.
- The organization may restrict or withdraw ಪ್ರವೇಶ where a ಭದ್ರತೆ ಅಪಾಯ is identified.
- Business ಮಾಹಿತಿ ತೆಗೆದುಹಾಕಬೇಕು from personal ಸಾಧನಗಳು when no longer authorized.

ಅನುಬಂಧ 06

ಭೌತಿಕ ಮತ್ತು ಪರಿಸರ ಭದ್ರತಾ ನಿಯಮಗಳು

ಉಲ್ಲೇಖ: FTS/ISIT/POL/01 – ಅನುಬಂಧ 06

Somindra ಸಂಸ್ಥೆಯು ರಕ್ಷಿಸು its ಕಚೇರಿ, ಉಪಕರಣಗಳು, ಮಾಹಿತಿ and other ಭೌತಿಕ assets against ಅನಧಿಕೃತ ಪ್ರವೇಶ, theft, damage and ಪರಿಸರೀಯ threats.

ಮುಖ್ಯ ನಿಯಮಗಳು

- Access to ಕಚೇರಿ premises ಬೇಕು ಸೂಕ್ತly controlled.
- Visitors ಬೇಕು ಸೂಕ್ತly managed.
- Visitors ಬಾರದು provided unrestricted ಪ್ರವೇಶ to sensitive areas or ಮಾಹಿತಿ.
- Computers and other ಉಪಕರಣಗಳು ಬೇಕು positioned to reduce unauthorized viewing or ಭೌತಿಕ damage.
- Employees ಬೇಕು follow clear-desk and clear-screen practices.
- Company laptops and ಉಪಕರಣಗಳು taken outside the ಕಚೇರಿ ರಕ್ಷಿಸಬೇಕು against ನಷ್ಟ and theft.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

- CCTV/ಭದ್ರತೆ ಉಪಕರಣಗಳು ಬೇಕು ಸೂಕ್ತly ರಕ್ಷಿಸು.
- Fire, electrical, water, ಪರಿಸರೀಯ and other ಭೌತಿಕ ಅಪಾಯಗಳು ಪರಿಗಣಿಸಬೇಕು.
- Equipment ನಿರ್ವಹಿಸಬೇಕು ಸೂಕ್ತly.
- Storage media and ಉಪಕರಣಗಳು ಬೇಕು securely disposed of or reಬಳಸಿದ after ಸೂಕ್ತ ದತ್ತಾಂಶ removal.

ಅನುಬಂಧ 07

IT ಸೇವಾ ನಿರ್ವಹಣೆ ಮತ್ತು ಸೇವಾ ಗುಣಮಟ್ಟದ ನಿಯಮಗಳು

ಉಲ್ಲೇಖ: FTS/ISIT/POL/01 – ಅನುಬಂಧ 07

Somindra ಸಂಸ್ಥೆಯು manage IT ಆಧಾರಿತ ಸೇವೆಗಳು in a structured and ಗ್ರಾಹಕ-focಬಳಸಿದ manner throughout the ಸೇವೆ lifecycle.

ಸೇವಾ ಜೀವನಚಕ್ರ

ಗ್ರಾಹಕರ ಅವಶ್ಯಕತೆ → ಯೋಜನೆ → ಖರೀದಿ → ಪೂರೈಕೆ → ಸ್ಥಾಪನೆ → ಕಾನ್ಫಿಗರೇಶನ್ → ಕಮಿಷನಿಂಗ್ → ಹಸ್ತಾಂತರ → ತಾಂತ್ರಿಕ ಬೆಂಬಲ → ಸೇವಾ ಮುಕ್ತಾಯ / ಸುಧಾರಣೆ

ಮುಖ್ಯ ನಿಯಮಗಳು

- Customer and ಸೇವಾ ಅವಶ್ಯಕತೆಗಳು ಬೇಕು clearly understood and recorded.
- Responsibilities for ಸೇವೆ delivery ನಿರ್ಧರಿಸಬೇಕು.
- Installation and ಕಮಿಷನಿಂಗ್ ಬೇಕು performed in accordance with approved ಅವಶ್ಯಕತೆಗಳು.
- Service requests and ಘಟನೆಗಳು ದಾಖಲಿಸಬೇಕು and tracked.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01 V.2.0, R.0.0 EFF DATE :21.08.2026
--	---	---

- Customer communication ಬೇಕು timely and ಸೂಕ್ತ.
- Changes affecting ಸೇವೆಗಳು ಬೇಕು ಸೂಕ್ತly assessed and authorized.
- Service ಕಾರ್ಯಕ್ಷಮತೆ ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಬೇಕು against defined ಅವಶ್ಯಕತೆಗಳು.
- Customer ಪ್ರತಿಕ್ರಿಯೆ and complaints ದಾಖಲಿಸಬೇಕು and addressed.
- Service records ನಿರ್ವಹಿಸಬೇಕು as evidence of delivery.
- Opportunities for improving ಸೇವೆ quality ಬೇಕು identified and acted upon.

ಅನುಬಂಧ 08

IT ಬದಲಾವಣೆ, ಕಾನ್ಫಿಗರೇಶನ್ ಮತ್ತು ಬಿಡುಗಡೆ ನಿಯಮಗಳು

ಉಲ್ಲೇಖ: FTS/ISIT/POL/01 – ಅನುಬಂಧ 08

Changes to IT ವ್ಯವಸ್ಥೆಗಳು, ಕಾನ್ಫಿಗರೇಶನ್‌s, ಸ್ಟಾಪನೆಸ್ and ಗ್ರಾಹಕ solutions ಬೇಕು controlled to minimize ಭದ್ರತೆ and ಸೇವೆ ಅಪಾಯಗಳು.

ಮುಖ್ಯ ನಿಯಮಗಳು

1. Changes ಬೇಕು identified and ಸೂಕ್ತly documented.
2. Changes ಪರಿಶೀಲಿಸಬೇಕು for potential ಮಾಹಿತಿ ಭದ್ರತಾ and ಸೇವೆ impacts.
3. Appropriate ಅನುಮೋದನೆ ಬೇಕು obtained before implementation.
4. Critical ಕಾನ್ಫಿಗರೇಶನ್‌s ದಾಖಲಿಸಬೇಕು where necessary.
5. Changes ಪರಿಶೀಲಿಸಬೇಕು or verified where practical.
6. Customer-impacting ಬದಲಾವಣೆಗಳು ತಿಳಿಸಬೇಕು ಸೂಕ್ತly.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01 V.2.0, R.0.0 EFF DATE :21.08.2026
--	---	---

7. Emergency ಬದಲಾವಣೆಗಳು ಬೇಕು controlled and ಪರಿಶೀಲನೆ after implementation.
8. Failed ಬದಲಾವಣೆಗಳು ಬೇಕು corrected or rolled back where practical.
9. Configuration records ಬೇಕು updated following ಸಂಬಂಧಿತ ಬದಲಾವಣೆಗಳು.
10. Unauthorized ಬದಲಾವಣೆಗಳು ಬೇಕು investigated.

ಅನುಬಂಧ 09

ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಸೈಬರ್ ಘಟನೆಗಳ ನಿಯಮಗಳು

ಉಲ್ಲೇಖ: FTS/ISIT/POL/01 – ಅನುಬಂಧ 09

All ಸಿಬ್ಬಂದಿ ಬೇಕು promptly ವರದಿ actual or suspected ಮಾಹಿತಿ ಭದ್ರತಾ and ಸೈಬರ್ ಭದ್ರತೆ ಘಟನೆಗಳು.

ಉದಾಹರಣೆಗಳು

- Phishing, suspicious emails, malware, ransomware or other malicious activities;
- Unಅಧಿಕೃತ ಪ್ರವೇಶ, ಪಾಸ್‌ವರ್ಡ್/credential compromise or unauthorized ವ್ಯವಸ್ಥೆ ಬದಲಾವಣೆಗಳು;
- Loss or theft of laptops, ಸಾಧನಗಳು, ಉಪಕರಣಗಳು or ಮಾಹಿತಿ;
- Accidental or unauthorized ಬಹಿರಂಗಪಡಿಸುವಿಕೆ, leakage or ನಷ್ಟ of confidential/ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ;
- Cyberಭದ್ರತೆ attacks, significant IT ಸೇವೆ disruptions or any other event that may compromise ಮಾಹಿತಿ ಭದ್ರತೆ or ಸೇವೆ ಲಭ್ಯತೆ.

ಘಟನೆಗಳ ನಿಯಮಗಳು

- Report ಘಟನೆಗಳು immediately through the defined ವರದಿing channel.
- Do not delete or alter ಸಂಬಂಧಿತ evidence unnecessarily.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

- Incidents ಬೇಕು assessed and classified according to severity.
- Appropriate containment and ಸರಿಪಡಿಸುವ ಕ್ರಮ ಬೇಕು initiated.
- Relevant ಗ್ರಾಹಕರು, ಪೂರೈಕೆದಾರರು or authorities ಬೇಕು informed where required.
- Incident records ನಿರ್ವಹಿಸಬೇಕು.
- Lessons learned ಪರಿಗಣಿಸಬೇಕು for preventing recurrence.

ಅನುಬಂಧ 10

ಬ್ಯಾಕಪ್, ವಿಪತ್ತು ಮರುಪಡೆಯುವಿಕೆ ಮತ್ತು ವ್ಯವಹಾರ ನಿರಂತರತಾ ನಿಯಮಗಳು

ಉಲ್ಲೇಖ: FTS/ISIT/POL/01 – ಅನುಬಂಧ 10

Somindra ಸಂಸ್ಥೆಯು maintain practical arrangements to ರಕ್ಷಿಸು critical ಮಾಹಿತಿ and continue or restore important business and IT ಆಧಾರಿತ ಸೇವೆಗಳು following disruption.

ಮುಖ್ಯ ನಿಯಮಗಳು

- Important business ಮಾಹಿತಿ ಬೇಕು backed up using approved arrangements.
- Backup arrangements ಬೇಕು consider ಗೌಪ್ಯತೆ, ಸಮಗ್ರತೆ and ಲಭ್ಯತೆ.
- Backup restoration ಪರಿಶೀಲಿಸಬೇಕು periodically where practical.
- Critical IT dependencies ಬೇಕು identified.
- Business ನಿರಂತರತೆ and ವಿಪತ್ತು ಮರುಪಡೆಯುವಿಕೆ arrangements ಬೇಕು address reasonably foreseeable disruptions.
- Employees ಬೇಕು understand their ಜವಾಬ್ದಾರಿಗಳು during significant disruption.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

- Recovery priorities ಬೇಕು based on business and ಸೇವಾ ಅವಶ್ಯಕತೆಗಳು.
- Lessons from disruptions and recovery exercises ಬಳಸಬೇಕು for ಸುಧಾರಣೆ.

ಅನುಬಂಧ 11

ಪೂರೈಕೆದಾರ, ಕ್ಲೌಡ್ ಮತ್ತು ತೃತೀಯ ಪಕ್ಷದ ಭದ್ರತಾ ನಿಯಮಗಳು

ಉಲ್ಲೇಖ: FTS/ISIT/POL/01 – ಅನುಬಂಧ 11

Somindra ಸಂಸ್ಥೆಯು consider ಮಾಹಿತಿ ಭದ್ರತಾ and IT ಸೇವಾ ಅವಶ್ಯಕತೆಗಳು when selecting and managing ಪೂರೈಕೆದಾರರು, OEMs, contractors, ಕ್ಲೌಡ್-ಸೇವೆ providers and other ತೃತೀಯ ಪಕ್ಷಗಳು.

ಮುಖ್ಯ ನಿಯಮಗಳು

- Relevant ಪೂರೈಕೆದಾರರು ಮೌಲ್ಯಮಾಪನ ಮಾಡಬೇಕು according to business and ಭದ್ರತೆ ಅಪಾಯ.
- Security and ಗೌಪ್ಯತೆ ಅವಶ್ಯಕತೆಗಳು ಸೇರಿಸಬೇಕು in agreements where ಸೂಕ್ತ.
- Supplier ಪ್ರವೇಶ to Somindra/ಗ್ರಾಹಕರ ಮಾಹಿತಿ ಸೀಮಿತಗೊಳಿಸಬೇಕು to authorized ಅವಶ್ಯಕತೆಗಳು.
- Cloud ಸೇವೆಗಳು ಬಳಸಬೇಕು in accordance with approved ವ್ಯವಹಾರ ಅವಶ್ಯಕತೆಗಳು.
- Supplier ಕಾರ್ಯಕ್ಷಮತೆ and ಸಂಬಂಧಿತ ಭದ್ರತೆ issues ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಬೇಕು.
- Supplier ಘಟನೆಗಳು affecting Somindra ಸೇವೆಗಳು or ಮಾಹಿತಿ ಪರಿಹರಿಸಬೇಕು.
- Supplier ಬದಲಾವಣೆಗಳು that may affect ಸೇವೆಗಳು or ಭದ್ರತೆ ಪರಿಶೀಲಿಸಬೇಕು.
- Third-party ಪ್ರವೇಶ ಹಿಂಪಡೆಯಬೇಕು when no longer required.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ಅನುಬಂಧ 12

ಭದ್ರತಾ ಜಾಗೃತಿ, ತರಬೇತಿ ಮತ್ತು ನಿರಂತರ ಸುಧಾರಣೆಯ ನಿಯಮಗಳು

ಉಲ್ಲೇಖ: FTS/ISIT/POL/01 – ಅನುಬಂಧ 12

Somindra ಸಂಸ್ಥೆಯು ensure that ಸಿಬ್ಬಂದಿ possess ಸೂಕ್ತ ಜಾಗೃತಿ and competence to perform their ಜವಾಬ್ದಾರಿಗಳು securely and effectively.

ಮುಖ್ಯ ನಿಯಮಗಳು

- New ಸಿಬ್ಬಂದಿ ಬೇಕು receive ಸೂಕ್ತ ಮಾಹಿತಿ ಭದ್ರತಾ and IT ಸೇವೆ ಜಾಗೃತಿ.
- Periodic ತರಬೇತಿ ಬೇಕು cover ಸಂಬಂಧಿತ ಸೈಬರ್ ಭದ್ರತೆ and ಸೇವೆ-ನಿರ್ವಹಣೆ topics.
- Training attendance ದಾಖಲಿಸಬೇಕು.
- Training effectiveness ಮೌಲ್ಯಮಾಪನ ಮಾಡಬೇಕು where ಸೂಕ್ತ.
- Personnel ಬೇಕು informed about significant ನೀತಿ or procedure ಬದಲಾವಣೆಗಳು.
- Security ಘಟನೆಗಳು, ಆಡಿಟ್ findings, ಸೇವೆ failures and ಗ್ರಾಹಕ ಪ್ರತಿಕ್ರಿಯೆ ಪರಿಗಣಿಸಬೇಕು for ಸುಧಾರಣೆ.
- Nonconformities ಪರಿಹರಿಸಬೇಕು through ಸರಿಪಡಿಸುವ ಕ್ರಮ.
- Relevant KPIs and objectives ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಬೇಕು.
- ನಿರ್ವಹಣೆಯು periodically ಪರಿಶೀಲನೆ ISMS and ITSM ಕಾರ್ಯಕ್ಷಮತೆ.
- ಸಂಸ್ಥೆಯು continually improve the effectiveness of its ನಿರ್ವಹಣೆ ವ್ಯವಸ್ಥೆಗಳು.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

ಅನುಬಂಧ 13

ಸುರಕ್ಷಿತ ಕೆಲಸ, ದತ್ತಾಂಶ ಸೋರಿಕೆ ತಡೆ, ಕ್ರಿಪ್ಟೋಗ್ರಫಿ ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್ ಭದ್ರತಾ ನಿಯಮಗಳು

ಉಲ್ಲೇಖ: SM/ISIT/POL/01 – ಅನುಬಂಧ 13

Somindra ಸಂಸ್ಥೆಯು establish practical ಭದ್ರತೆ ಅವಶ್ಯಕತೆಗಳು for work performed in secure areas, prevention of unauthorized ಮಾಹಿತಿ leakage, ಸೂಕ್ತ ಬಳಕೆ of cryptography and ಭದ್ರತೆ ಅವಶ್ಯಕತೆಗಳು for ಅಪ್ಲಿಕೇಶನ್‌ಗಳು and technology solutions. These ನಿಯಮಗಳು supplement the existing Physical & Environmental Security Rules, Remote Working & BYOD Rules, Information Classification, Privacy & Data Protection Rules, Access Control & Authentication Rules, IT Change, Configuration & Release Rules, Backup, Disaster Recovery & Business Continuity Rules, and Supplier, Cloud & Third-Party Security Rules.

A. ನಿಯಂತ್ರಿತ / ಸುರಕ್ಷಿತ ಪ್ರದೇಶಗಳಲ್ಲಿ ಸುರಕ್ಷಿತ ಕೆಲಸ

- Access to sensitive or critical areas ಸೀಮಿತಗೊಳಿಸಬೇಕು to ಅಧಿಕೃತ ಸಿಬ್ಬಂದಿ based on business need.
- Visitors, vendors and ತೃತೀಯ ಪಕ್ಷಗಳು ಬಾರದು enter controlled or restricted areas without ಅನುಮೋದನೆ and ಸೂಕ್ತ supervision.
- Sensitive documents, screens, removable media and ಉಪಕರಣಗಳು ಬಾರದು left exposed or unattended.
- Photography, video/audio recording or ಬಳಕೆ of personal recording/ಸಂಗ್ರಹಣೆ ಸಾಧನಗಳು in restricted areas ಬಾರದು permitted unless specifically authorized.
- Portable computers, ಸಂಗ್ರಹಣೆ media and other ಸಾಧನಗಳು ಬಳಸಿದ in controlled areas ಬೇಕು subject to ಅನ್ವಯವಾಗುವ ಭದ್ರತೆ controls.
- Doors and ಪ್ರವೇಶ points to controlled areas ಬಾರದು bypassed or intentionally left unsecured.
- Unauthorized entry, ನಷ್ಟ, tampering or other ಭೌತಿಕ-ಭದ್ರತೆ concerns ಬೇಕು ವರದಿ ಮಾಡಲಾಗಿದೆ promptly.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

B. ದತ್ತಾಂಶ ಸೋರಿಕೆ ತಡೆ

- Information ಬೇಕು ಪ್ರವೇಶದ, copied, downloaded, ವರ್ಗಾಯಿಸಿದ or shared only for authorized ವ್ಯವಹಾರ ಉದ್ದೇಶಗಳು and in accordance with its classification.
- Confidential or restricted ಮಾಹಿತಿ ಬಾರದು ಬಹಿರಂಗಪಡಿಸಿದ or ವರ್ಗಾಯಿಸಿದ through unauthorized channels.
- Customer, ಪೂರೈಕೆದಾರ, commercial, technical, financial and ಒಪ್ಪಂದಾತ್ಮಕ ಮಾಹಿತಿ ಬೇಕು shared externally only with ಸೂಕ್ತ ಅನುಮೋದನೆ and safeguards.
- Personal email, personal ಕೌಡ್ ಸಂಗ್ರಹಣೆ, unauthorized file-sharing ಸೇವೆಗಳು and removable media ಬಾರದು ಬಳಸಿದ for Somindra or ಗ್ರಾಹಕರ ಮಾಹಿತಿ unless specifically authorized.
- Unnecessary local copies, downloads and duplicate ಸಂಗ್ರಹಣೆ of sensitive ಮಾಹಿತಿ ತಪ್ಪಿಸಬೇಕು.
- Information ಬೇಕು securely deleted or disposed of when no longer required, subject to ಅನ್ವಯವಾಗುವ retention ಅವಶ್ಯಕತೆಗಳು.
- Suspected ಮಾಹಿತಿ leakage, accidental ಬಹಿರಂಗಪಡಿಸುವಿಕೆ, ನಷ್ಟ or unauthorized ವರ್ಗಾವಣೆ ತಕ್ಷಣ ವರದಿ ಮಾಡಬೇಕು.
- Where technically feasible, available email, ಕೌಡ್, endpoint and ಪ್ರವೇಶ-control ಭದ್ರತೆ features ಬಳಸಬೇಕು to reduce the ಅಪಾಯ of unauthorized ಬಹಿರಂಗಪಡಿಸುವಿಕೆ.

C. ಕ್ರಿಪ್ಟೋಗ್ರಫಿಯ ಬಳಕೆ

- Cryptographic ರಕ್ಷಣೆ ಬಳಸಬೇಕು where required by ಮಾಹಿತಿ sensitivity, ಅಪಾಯ, ಒಪ್ಪಂದಾತ್ಮಕ ಅವಶ್ಯಕತೆಗಳು, ಅನ್ವಯವಾಗುವ law or ಸೇವಾ ಅವಶ್ಯಕತೆಗಳು.
- Confidential or sensitive ಮಾಹಿತಿ ರಕ್ಷಿಸಬೇಕು using ಸೂಕ್ತ encryption or other cryptographic safeguards when ಸಂಗ್ರಹಿಸಿದ or transmitted, where ಅನ್ವಯವಾಗುವ.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)

 SOMINDRA MARKETING	ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ	FORMAT. No :SM/ISIT/POL/01
		V.2.0, R.0.0
		EFF DATE :21.08.2026

- Passwords, encryption keys, recovery codes, ದೃಢೀಕರಣ secrets and other cryptographic credentials ರಕ್ಷಿಸಬೇಕು from ಅನಧಿಕೃತ ಪ್ರವೇಶ.
- Cryptographic keys and credentials ಬಾರದು shared insecurely or ಸಂಗ್ರಹಿಸಿದ in openly ಪ್ರವೇಶೀಯ locations.
- Security and encryption ಅವಶ್ಯಕತೆಗಳು ಪರಿಗಣಿಸಬೇಕು when using ಕ್ಲೌಡ್, SaaS, OEM and other ತೃತೀಯ ಪಕ್ಷದ ಸೇವೆಗಳು.
- Access to credentials and cryptographic keys ಬಳಸಿದ to ರಕ್ಷಿಸು Somindra or ಗ್ರಾಹಕರ ಮಾಹಿತಿ ಬೇಕು restricted to ಅಧಿಕೃತ ಸಿಬ್ಬಂದಿ.

D. ಅಪ್ಲಿಕೇಶನ್ ಮತ್ತು ಸಾಫ್ಟ್‌ವೇರ್ ಭದ್ರತಾ ಅವಶ್ಯಕತೆಗಳು

- Information-ಭದ್ರತೆ ಅವಶ್ಯಕತೆಗಳು ಪರಿಗಣಿಸಬೇಕು before acquiring, supplying, configuring, installing or materially changing ಅಪ್ಲಿಕೇಶನ್‌ಗಳು and technology solutions.
- Only approved, licensed and authorized ಸಾಫ್ಟ್‌ವೇರ್ and ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಬಳಸಬೇಕು on organizational ಸಾಧನಗಳು and ವ್ಯವಸ್ಥೆಗಳು.
- Third-party and OEM ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಬೇಕು assessed, as ಸೂಕ್ತ, for ಭದ್ರತೆ, ಪ್ರವೇಶ, support, licensing, update, compatibility and ಒಪ್ಪಂದಾತ್ಮಕ ಅವಶ್ಯಕತೆಗಳು.
- Application ಪ್ರವೇಶ ಬೇಕು restricted according to business need and assigned ಜವಾಬ್ದಾರಿಗಳು.
- Security updates, patches and ಕಾನ್ಫಿಗರೇಶನ್ ಬದಲಾವಣೆಗಳು ಬೇಕು implemented or coordinated based on ಅಪಾಯ, OEM guidance and ಸೇವಾ ಅವಶ್ಯಕತೆಗಳು.
- Applications and ಕಾನ್ಫಿಗರೇಶನ್‌s ಪರಿಶೀಲಿಸಬೇಕು or verified before deployment where practical, particularly where ಗ್ರಾಹಕರ ಮಾಹಿತಿ, ಭದ್ರತೆ or ಸೇವೆ ಲಭ್ಯತೆ may be affected.
- For ಸಾಫ್ಟ್‌ವೇರ್ and solutions supplied, installed, configured or commissioned by Somindra, ಅನ್ವಯವಾಗುವ ಭದ್ರತೆ ಅವಶ್ಯಕತೆಗಳು ಪರಿಗಣಿಸಬೇಕು during ಖರೀದಿ, ಸ್ಥಾಪನೆ, ಕಾನ್ಫಿಗರೇಶನ್, testing and handover.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)



SOMINDRA MARKETING

ಸಂಯೋಜಿತ ಮಾಹಿತಿ ಭದ್ರತೆ ಮತ್ತು ಐಟಿ
ಸೇವಾ ನಿರ್ವಹಣಾ ನೀತಿ

FORMAT. No :SM/ISIT/POL/01

V.2.0, R.0.0

EFF DATE :21.08.2026

- Security weaknesses, unauthorized ಸಾಫ್ಟ್‌ವೇರ್, unsupported ಅಪ್ಲಿಕೇಶನ್‌ಗಳು or significant ಅಪ್ಲಿಕೇಶನ್-ಭದ್ರತೆ concerns ಪರಿಹರಿಸಬೇಕು through the ಅನ್ವಯವಾಗುವ ಅಪಾಯ, ಘಟನೆ, ಪೂರೈಕೆದಾರ or ಬದಲಾವಣೆ-ನಿರ್ವಹಣೆ process.

E. ಜವಾಬ್ದಾರಿ ಮತ್ತು ಜಾಗೃತಿ

- Personnel ಬೇಕು comply with these ನಿಯಮಗಳು and ರಕ್ಷಿಸು Somindra and ಗ್ರಾಹಕರ ಮಾಹಿತಿ, ವ್ಯವಸ್ಥೆಗಳು, ಸಾಧನಗಳು and other assets.
- The CISO and ನಿರ್ವಹಣೆಯು ensure ಜಾಗೃತಿ of these ಅವಶ್ಯಕತೆಗಳು through the existing ISMS/ITSM ತರಬೇತಿ and ಜಾಗೃತಿ programme.
- Violations or repeated non-compliance ಪರಿಹರಿಸಬೇಕು through the ಅನ್ವಯವಾಗುವ ಘಟನೆ, disciplinary, corrective-action or ಒಪ್ಪಂದಾತ್ಮಕ process.

ದಾಖಲೆ ಬದಲಾವಣೆ ಟಿಪ್ಪಣಿ			
ಆವೃತ್ತಿ ಸಂಖ್ಯೆ	ಪರಿಷ್ಕರಣೆ ಸಂಖ್ಯೆ	ಜಾರಿಗೆ ಬಂದ ದಿನಾಂಕ	ಬದಲಾವಣೆಗಳ ಸಾರಾಂಶ
01	00	01.08.2026	ಮೊದಲ ಬಿಡುಗಡೆ
02	00	21.08.2026	ಸುರಕ್ಷಿತ ಕೆಲಸ, ದತ್ತಾಂಶ ಸೋರಿಕೆ ತಡೆ, ಕ್ರಿಪ್ಟೋಗ್ರಫಿ ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್/ಸಾಫ್ಟ್‌ವೇರ್ ಭದ್ರತಾ ಅವಶ್ಯಕತೆಗಳನ್ನು ನಿರ್ಧರಿಸಲು Stage 1 AOCs ನಂತರ ಅನುಬಂಧ 13 ಅನ್ನು ಪರಿಚಯಿಸಲಾಗಿದೆ.

ತಯಾರಿಸಿದವರು: ಭೀಮನಗೌಡ ಪಾಟೀಲ್ (CISO)

ಅನುಮೋದಿಸಿದವರು: ಮೋಹನ್ ಎಸ್. ದೇಸಾಯಿ (MD)