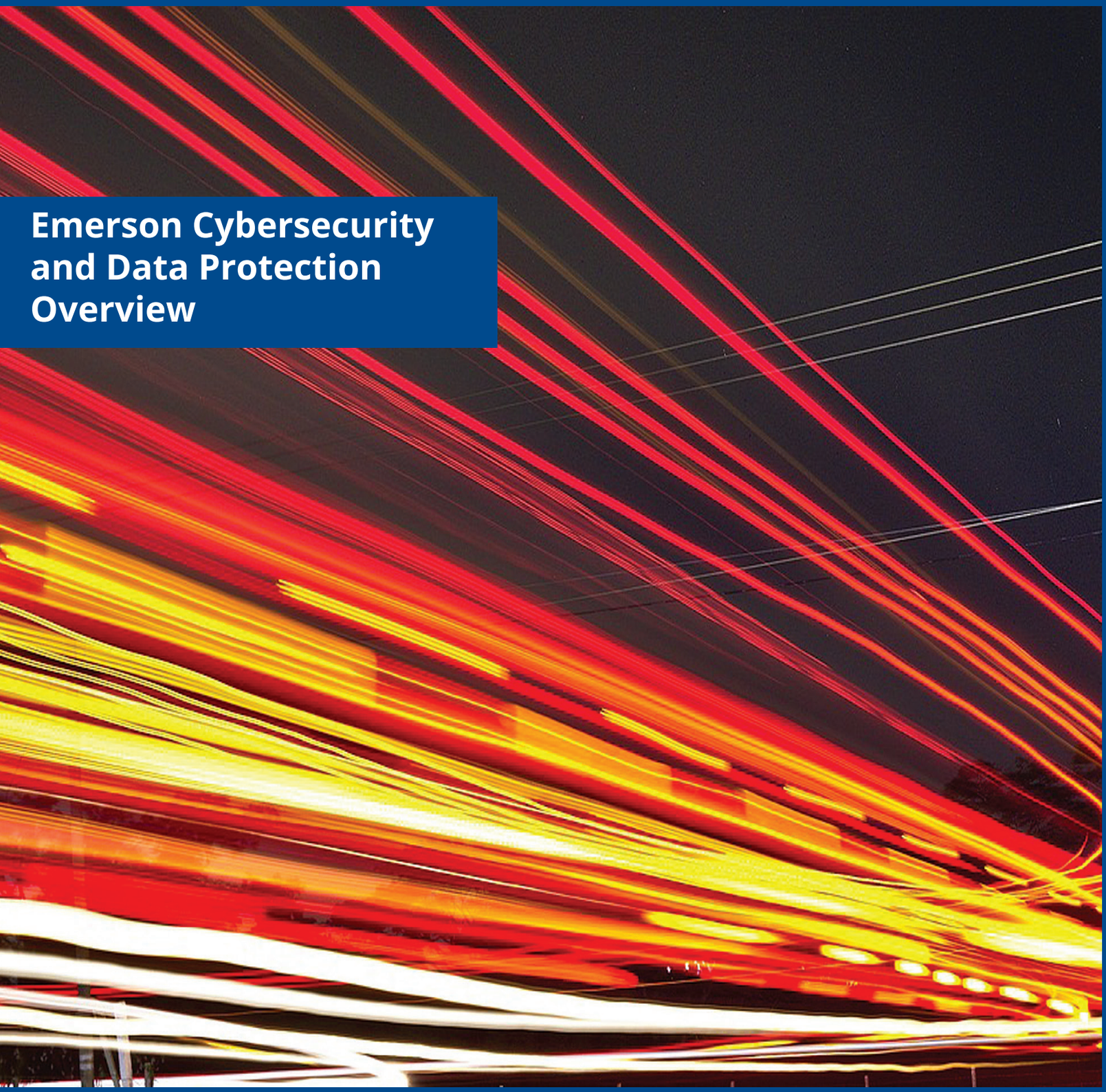
Emerson Cybersecurity and Data Protection Overview



Unleash boundless automation with intelligent field, edge and cloud computing developed to be secure, and sustainable

EMERSON

Expertise, technology and services that keep your operations running smoothly and securely

You can facilitate digital transformation and drive improvement across your organization by leveraging Emerson technologies that reduce your operations risk and empower your workforce with knowledge, behaviors and tools to help protect your operations from cyber threats.

Emerson's industry expertise, consulting services and comprehensive software and technologies help manufacturers maximize production, protect people and the environment while optimizing energy and reducing operating costs for industries around the world.

Purpose

The purpose of this document is to provide an overview of Emerson's Corporate IT security practices that are in effect as of this document's published date.

Emerson customers who leverage or want to leverage Emerson Corporate IT network and/or security services may use this document as a primer to understand the elements of Emerson's security program.

External parties can leverage this high-level document to ask more specific questions about Emerson's security controls, policies, tools, etc.

Terms

The scope of the technical and application information is limited and is subject to updates, without notice, as we constantly evaluate and improve our technologies and as capabilities expand. The service you receive as a customer and your privacy are important to us. We take measures to safeguard your system and to protect your data. In order to provide you with our services, information is collected in accordance with our Emerson website terms, available at:

https://www.emerson.com/en-us/privacy-notice

https://www.emerson.com/en-us/terms-of-use

https://www.emerson.com/en-us/cookie-notice

This document is enterprise wide, note that additional terms and conditions may apply to specific products (including but not limited to: Warranty, Terms of Service, Product Privacy, Subscription Terms).

Emerson Data Protection Statement

Emerson is committed to protecting the personal information of its customers, employees, vendors, and investors, all of whom expect us to adhere to the highest standards of data privacy and security. Emerson first implemented a formal Data Protection Program to keep pace with the rigorous requirements of the European Union (EU) Data Protection Directive. Over time, the data privacy and security landscape has experienced an unprecedented and rapid level of change in technology, regulations, and stakeholder expectations.

To respond to this changing environment, Emerson undertook to inventory its Data Protection systems, processes, and controls. These efforts resulted in the re-design and implementation of a Global Data Protection Program enabling Emerson to stay abreast of key data privacy and security developments across the globe, and to adapt our global operations to remain compliant in this shifting landscape.

Emerson's Global Data Protection Program requires all Emerson businesses, wherever located, to adhere to the core data handling and documentation requirements of the European General Data Protection Regulation (GDPR). Emerson's program is supported by an updated Data Protection Policy, the establishment of a cross functional management advisory board, and the appointment of local and functional data protection coordinators around the world.

Emerson has expanded its Global Data Protection program meet the challenges presented by the proliferation of data protection legislation around the world such as the California Consumer Privacy Act (CCPA), the Brazilian General Data Protection Law, and the India Data Privacy Bill – all of which borrow considerably from the GDPR. In addition, Emerson implemented a rigorous product security policy requiring secure product development and product privacy and security risk review at all Emerson businesses.

The GDPR, CCPA, and other new regional and local laws change the way companies like Emerson must administer and document the collection, movement, and processing of personal data. While data regulations are dynamic, they do not change the fundamental principles upon which Emerson has historically relied on to manage personal data. Emerson's Global Data Protection Program will remain measured and nimble to maintain a strong, effective, and sustainable program that will be able to mature and adapt to future regulatory developments and our stakeholders' needs. Emerson has and will continue to place keen emphasis on the importance of keeping personal data secure and respecting the privacy rights of individuals around the world.

Last Revised: August 2023

Information Security Policies and Standards

Emerson maintains a comprehensive information security program, which includes policies, standards, procedures and guidelines. The information security program is informed by several industry-standard guidelines and best practices including ISO27001, NIST CSF, and DFARS.

Emerson's IT leadership meets on a regular basis to consider strategic and tactical direction for the information security program, and its policies, standards, procedures and guidelines.

Cybersecurity

Emerson's Chief Information Security Officer (CISO) oversees Emerson's Cybersecurity program. This responsibility includes the following areas:

- **Awareness and Training**
- **Cloud and Third-Party Risk Assessments**
- **Data Analytics and Automation**
- **Data Privacy and Protection**
- **Governance, Risk Management and Compliance**
- **Identity and Access Management**
- **Incident Response and Intelligence**
- **Insider Threat and Investigative Support**
- **Threat and Vulnerability Management**
- **Connected Products**

The cybersecurity programs are supported by the technical expertise of the above-mentioned teams within the IT organization, facility support and other experts as required. The businesses are responsible for implementing procedures specific to their products and services, where different local and industry regulatory requirements come into play. Emerson also engages third-party expertise to help ensure it maintains a current view of evolving issues in the areas of data privacy, risk and security on a global basis.

Risk Management

Emerson's risk management program monitors for possible threats and vulnerabilities to information technology assets. Risk assessments are performed regularly and when there are significant changes to infrastructure, technology, or other factors.

ISO 27001

To help customers and suppliers understand Emerson's security posture, Emerson certifies the information security program through ISO 27001. This certification specifies the requirements for establishing, implementing, maintaining, and continually improving Emerson's information security program. Today, Emerson's Global Data Center and Regional Data Centers are ISO 27001 certified. For more information regarding Emerson's ISO 27001 certified locations, please contact us.

Cyber Maturity Assessment

An independent external entity assesses the maturity of Emerson's cybersecurity program regularly and measures program maturity against industry peers and industry standards such as NIST Cybersecurity Framework and other common frameworks. The security team discusses recommendations with executive leadership and the board of directors.

Penetration Tests

Emerson performs penetration tests of internal and external network infrastructure as well as connected products on ad hoc basis using dedicated internal staff specially trained and experienced in industry standard penetration test scopes and methods. In addition to the continuous efforts of Emerson's vulnerability management team conducting penetration testing, Emerson engages in regular external penetration exercises using an industry-leading third-party. Results are reviewed by the Information Security organization and action is taken based on risk.

Awareness

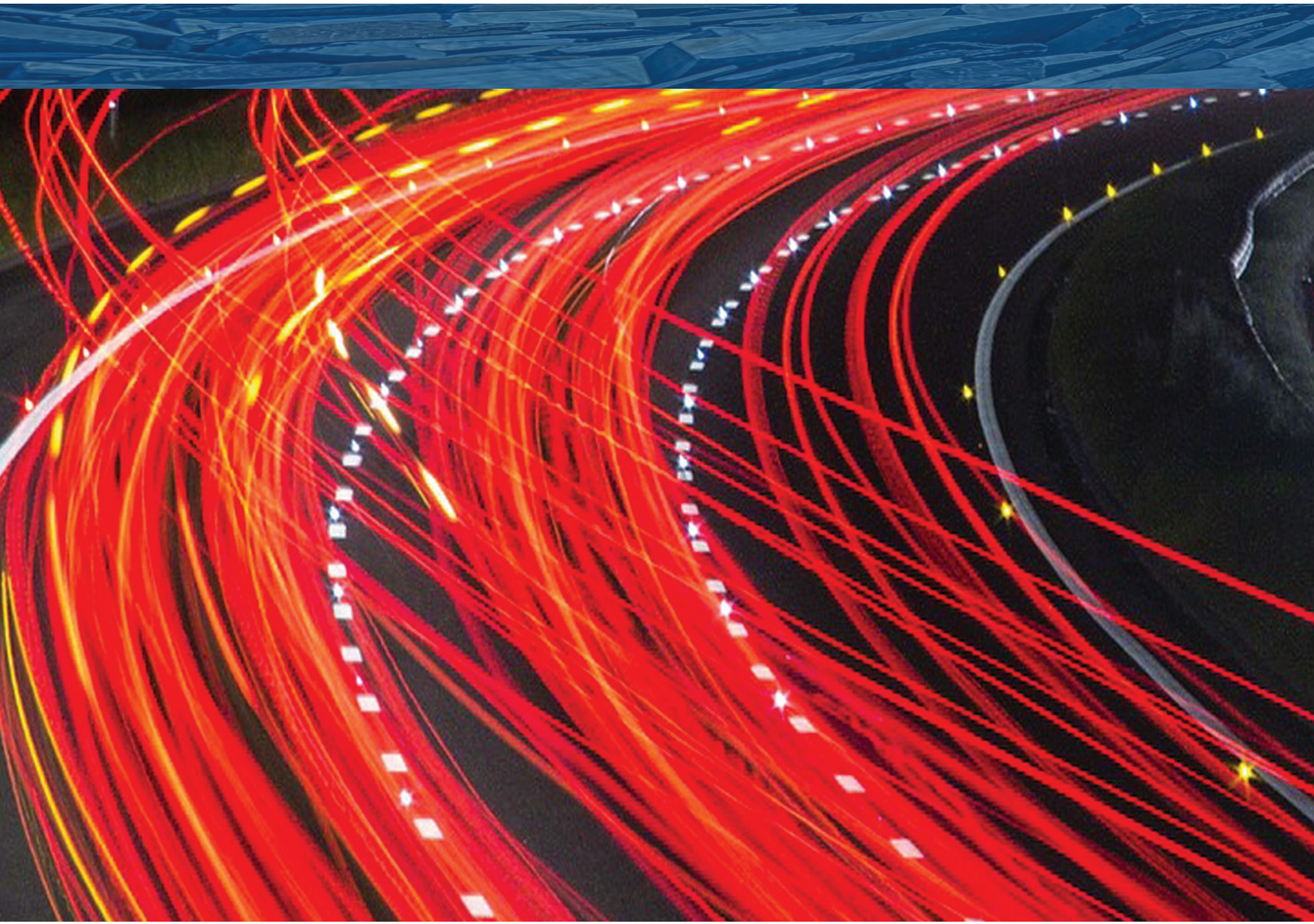
All Emerson employees are required to complete an information security training that covers end-user security risks. Emerson's security awareness training includes subjects such as Emerson's security policy, data classification and handling, workspace and desktop security, network security (VPN), password security, phishing, malware, file sharing, clean desk, and many others. In addition to awareness training, Emerson also actively tests (e.g. mock-phishing) employees to maintain end user diligence.

Data Protection

Emerson has a data classification policy in place. Data is classified into four categories: Public, Internal Use Only, Confidential, and Restricted. These classifications are based on the value and risk factors of the information. Security handling and control standards have been defined for information in each of the categories. These security precautions are defined for electronic files and information (at rest and in motion) and hard copies for each stage of the data management lifecycle.

Compliance and Privacy

Emerson's Legal & Compliance teams monitor and review relevant regulatory developments within their world regions or jurisdictions. Internal reviews include an assessment of the impact of regulatory developments and necessary compliance actions. Further reporting is done on these developments on a risk-based approach using existing risk management processes and structures. Emerson is committed to complying with data privacy regulations (e.g. the General Data Privacy Regulation and others) and is protecting customers, employees, and Emerson information.



Identity & Access Management

Emerson's Access Management policy identifies the requirements for controlling access to all Emerson information assets. Access is authorized based on the concepts of need-to-know and least-privilege and is defined by job role. User accounts (i.e. user IDs) and other access privileges for the Company's employees are created and revoked only after appropriate requests are made in conjunction with HR on-boarding and termination processes. Procedures allow for modification of user access in the event of job role or employment changes and for emergency revocation when circumstances require, such as in the case of involuntary terminations.

Administrative Accounts

Access to accounts with elevated privileges is restricted to authorized employees who require such access to perform their job functions. Server administrators have an administrative (admin) account that is separate from their normal user accounts. Admin accounts are centrally managed via Emerson Corporate IT's Privilege Access Management (PAM) solution. Access to the PAM requires multi-factor authentication. The privileged account credentials managed in PAM are routinely randomized. Admin accounts are reviewed quarterly.

Remote Access

Employee remote access to the Company's network is permitted and provided through a virtual private network (VPN) using two-factor authentication (user credentials and hard or soft token). Remote authentication to network devices (routers, switches, firewalls, etc.) is managed through a centralized server (Terminal Access Controller Access-Control System). Remote access is disabled for administrative accounts. Third-Party access or interfaces must meet Emerson standards and approvals. Access to third-parties is granted subject to risk assessment and appropriate contract terms and conditions.

Every Emerson employee is required to complete information security training

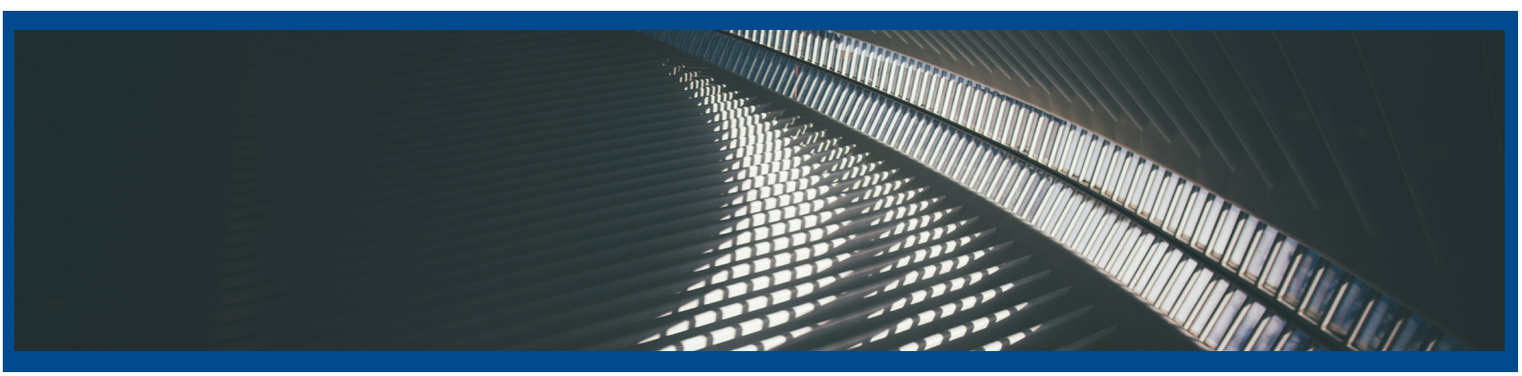
Incident Response, Intelligence, Analytics, and Investigative Support

Emerson has an incident response team and security monitoring team with access to advanced threat detection tools and an established incident management process to identify, document and address security incidents in a timely manner. The incident response process is updated regularly or when vendor or technology changes occur.

Vulnerability Management

A dedicated vulnerability management team tests Emerson's internal network regularly and external facing system hosted within Emerson data centers regularly and as-needed. Test outputs provide a granular view of system configurations (e.g., operating systems, open ports, running services) and are designed to detect known security vulnerabilities as well as backdoors and other malicious applications.

Emerson maintains a vulnerability management program that includes server hardening, scanning, alerting, and security and operating system patch management. Vendor and industry-accepted alert lists are monitored for new patches. Patches are reviewed at regularly scheduled meetings and are rated for deployment based on assessed severity levels. Emergency patch management meetings are called when needed. Security vulnerabilities and emerging threats are tracked by information security personnel, assessed by technical experts, and deployed according to risk priority.



Disaster Recovery and Business Continuity

Emerson has dedicated business resiliency and disaster recovery teams that coordinate Emerson's capability to recover systems using internal or external resources. Solutions are designed to meet requirements defined by impact analyses of system or facility outages. Where appropriate, human or computer workload is distributed among multiple locations to reduce or eliminate downtime due to local outages.

Tests are conducted regularly that may include, but are not be limited to: table top exercises, employee/all colleague call list tests, business disruption and relocation tests, and application recovery tests. The Company's network infrastructure is designed for high availability, with dual diverse, high bandwidth network links, that connect offices to the production data centers.

Critical applications are designed for high availability, using clustering or load balancing technology. Disaster recovery strategies are implemented based on business-defined requirements, including near time replication, delivering recovery in the optimum of time, with little to no loss of data.

Third-Party Security

Emerson assesses, monitors and manages its risk exposure from third-parties that provide IT products and services, or that have access to enterprise information. A global process exists to determine security implications and control requirements prior to entering into third-party agreements or allowing connectivity or access to Emerson information systems and information. Third-Parties and suppliers are also contractually required to maintain appropriate information security and confidentiality protections.

Physical and Environmental Security

Only authorized personnel with an Emerson issued electronic badge are granted access to Emerson's data centers. Emerson data centers are further restricted to only those personnel with the *need to access* restricted areas. Procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the data center facilities.

Human Resources Security

Upon hire, all personnel agree to comply with Emerson's policies, including those relating to information security, confidentiality and privacy. In addition, all Emerson personnel are required to complete security awareness training during the new hire onboarding process.

Emerson generally requires that background investigations be conducted for partners, principals and all employees at the time that they join Emerson. Potential issues that are identified in the background investigation are reviewed on an individual case-by-case basis, in light of guidance from applicable authorities. This individualized assessment includes a determination of whether the issues identified are job-related or pose a risk to Emerson or to its employees, partners, principals, or clients.

Your Trusted Partner to Securely Transform

About Emerson

Emerson (NYSE: EMR) is a global technology and software company providing innovative solutions for the world's essential industries. Through its leading automation portfolio, including its majority stake in AspenTech, Emerson helps hybrid, process and discrete manufacturers optimize operations, protect personnel, reduce emissions and achieve their sustainability goals. For more information, visit Emerson.com.

Go Boldly™

Emerson.com

© 2023 Emerson. All rights reserved.

The Emerson logo is a trademark and service mark of Emerson Electric Co. All other marks are the property of their respective owners.
The contents of this publication are presented for information purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the design or specifications of our products at any time without notice. Responsibility for proper selection, use and maintenance of any product remains solely with the purchaser and end user.

EMERSON™