Cybersecurity Site Policies and Procedures Development Service

- An essential part of a defense-in-depth strategy to limit cyber-breaches
- Economic results by reducing plant downtime
- Our consultants provide the right insight and advice to fine tune your site's cyber policies and procedures

Introduction

Safety policies are enforced from the moment that you enter the plant's front gate. Fail to comply with those policies and you may find yourself back outside those gates, looking in. Why, then, would you not approach cybersecurity with similar enforcement? The ramifications of not having appropriate cybersecurity policies and procedures in place and enforced are as great or greater than possible ramifications of safety infraction. When was the last time that a complete review of your existing site cybersecurity policies and procedures was conducted? It is reasonably safe to say that most sites do not regularly review and update these policies and procedures.

The Emerson Lifecycle Services Cybersecurity Site Policies and Procedures Development Service Team is ready to help you take your cybersecurity protection to the next level by systematically improving the cyber-related policies and procedures at your site(s). Our consultants provide the expertise and tools to review your current site policies and procedures and provide improvement suggestions to meet today's industry best practices.

Benefits

An essential part of a defense-in-depth strategy to limit cyber-breaches: A strong cybersecurity policy sets the security tone for the whole plant site and informs personnel about management's cybersecurity expectations. All personnel must be aware of the sensitivity of their potential impact on a plant's cybersecurity and their responsibilities for protecting it.

Economic results by reducing plant downtime: Effective and updated cybersecurity policies and procedures, along with proper enforcement, can help to avoid system downtime expenses due to a cyber-attack. Lost production revenue as well as recovery expenses from a single cyber-event will most certainly hit your plant's balance sheet and can often be avoided.

Our cybersecurity consultants provide the right insight and advice to fine tune your site's cyber policies and procedures: Policy and procedure review and/or development can be a time-consuming effort for even the savviest site specialist. With our certified consultants leading the development effort, you can be assured that the most current and effective enhancements will be included in your final policies and procedures manual.

EMERSON

Service Description

Building a cybersecurity program upon a solid foundation is necessary for success. The Emerson Cybersecurity Site Policies and Procedures Development Service offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to cybersecurity, our team identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. Emerson's professional services team consists of recognized security experts and authors with broad security experience with multinational corporations.

General Policy Creation Guidelines

Regardless of the topic of a particular security policy, certain key considerations should be made during its creation. Policies must require the establishment and maintenance of written security operational procedures. Policies must also identify required security plans for vital functions such as information security incident response, disaster recovery, or business continuity.

Compliance and Exceptions

The site's policies and procedures should address compliance and exceptions. Some organizations avoid writing a strong policy statement fearing a state of non-compliance with their own policy. An ideal policy issues strong clauses and addresses exceptions and enforcement. Failure to follow the policy without an authorized exemption should have consequences to ensure maximum cybersecurity effectiveness.

Deliverables

The Emerson Cybersecurity Site Policies and Procedures Development Service engagement includes:

- Initial teleconferencing of security consultant(s) to begin understanding your situation;
- Dispatch of security consultant(s) to your site;
- Review of current policies and procedures, including current use, enforcement and training;
- Stakeholder interviews including documented summary notes;
- Revised policies and procedures document;
- Gap-analysis document, if needed; and
- Management summary presentation.

Scope

A typical engagement ranges from one to four weeks depending on the number of policies and procedures involved. Investigations with a large number of policies and procedures may require more time. During the review and development phase, we collaborate closely with your security team, process control team, legal and compliance teams, among others.

At the completion of the review and development phase, a comprehensive report of findings as well as the new or revised policies and procedures manual will be delivered.

Ordering Information

Description	Model Number
Cybersecurity Site Policies & Procedures Development Service	Contact your Local Emerson Services Representative

Other Related Cybersecurity Services

- Cybersecurity Incident Response and Forensic Investigation Service
- Cybersecurity Incident Response Plan Development Service
- Cybersecurity Assessment Service
- Cybersecurity Remediation Service
- Integrated Patch Management Service
- Backup and Recovery Service
- Other DeltaV Cybersecurity Application Solutions include:
  - Endpoint Security For DeltaV Systems
  - Application Whitelisting for DeltaV Systems
  - Security Information and Event Management for DeltaV Systems
  - Network Security Monitor for DeltaV Systems
  - Threat Monitoring Solutions for DeltaV Systems

This product and/or service is expected to provide an additional layer of protection to your DeltaV system to help avoid certain types of undesired actions. This product and/or service represents only one portion of an overall DeltaV system security solution. Emerson does not warrant that the product and/or service or the use of the product and/or service protects the DeltaV system from cyber-attacks, intrusion attempts, unauthorized access, or other malicious activity ("Cyber Attacks"). Emerson shall not be liable for damages, non-performance, or delay caused by Cyber Attack. Users are solely and completely responsible for their control system security, practices and processes, and for the proper configuration and use of the security products.

To learn more, contact your local Emerson sales office or representative, or visit **www.emerson.com/deltavcybersecurity**.

Contact Us
www.emerson.com/contactus

EMERSON™