Policy number:	SL-POL-006.010	Revision number:	N/A
Original effective date:	Nov. 17, 2022	Pages:	18
Revised effective date:	N/A	Reviewed date:	N/A

SOLENIS POLICY
Operational Technology Security

1.0 Purpose

Solenis has a responsibility to establish a reasonable level of protection for its employees, assets, processes and information. A balanced approach of employee commitment, operational procedures, and manual and technical controls will achieve an appropriate level of security without unnecessarily restricting or impeding business or operational activities. A risk-based approach will determine minimum security standards that must be deployed at Solenis facilities. Additional security standards and safeguards may be required based on an assessment of possible threats and vulnerabilities, including a review of past incidents at the facility and surrounding area.

1.1 Table of contents

2.0 Scope

The guidelines in this document have been designed to provide a formal, adopted policy which specifies the baseline requirements for all Operational Technology (OT) assets, to be implemented across all company-owned and leased properties and any subsidiary properties and operating sites, occupied and unoccupied, and is enforceable to the outermost controllable perimeter of the property.

Due to the variety of possible physical characteristics, demographic factors, technologies deployed, risk factors and other environmental factors, this policy is by no means all inclusive. Rather, it sets the minimum requirements unless superseded by existing law and any exceptions would require Solenis Enterprise Risk and Security Management approval.

- All OT (Operational Technology) Systems – OT Systems will be used as a general term for all computing systems and technology used for Solenis plant operations and manufacturing. This includes, but is not limited to ICS (Industrial Control Systems), Distributed Control System (DCS), PCS (Process Control Systems), and PLC (Programmable Logic Controller) networks.
- The scope generally includes all non-business IT systems, networked or, connected or air gapped, at all Solenis plant sites

3.0 Audience

The intended audience and specific teams for which this policy is scoped is outlined in this section.

Corporate

Corporate teams are centrally responsible for all Solenis assets and personnel including: IT systems networked or connected to Solenis business environment, installation and maintenance of infrastructure, and related operations.

- **Executive team (CIO, COO, CISO roles)** is responsible for establishing the strategic direction for OT Security Program; identifying and examining new security controls; advising business operations managers, plant managers, and others with security management responsibilities to assist in the deployment of security controls; ensuring the use of appropriate technology; and developing security standards as they relate to security systems.
- **Infrastructure and Operations team** provides IT support for security system installations (including but not limited to SIEM technology, log consolidation and analysis tools, endpoint protection, network and computational infrastructure) as well as ongoing operation of the systems. The Infrastructure and Operations team also includes following functions
  - Identity and Access — to manage access rights and privileges across corporate and business assets
  - Network Engineering— responsible for deploying firewalls to plant sites and providing support for corporate network security products that can assist in providing more visibility into plant networks
  - Regional Infrastructure and Operations support — to provide support for local installation of security software or hardware and act as a liaison between local plant support teams and requirement from corporate teams.
- **Solenis Digital Security Team** provides support for security system configurations per Solenis policies and for responding to any potential cybersecurity incidents affecting the confidentiality, integrity, or availability of operational technology. The Digital Security Team includes Incident Management function that is responsible for managing and supervising security incident identification and response activities.

Operational Technology (OT)

Plant OT teams are responsible for OT systems (including, but not limited to, ICS, DCS, PCS and PLC networks) and related infrastructure, operations and maintenance within their

respective plant(s) / region and rely on support from respective corporate segments for installations, configuration, maintenance and incident resolution per policy requirements.

- **Plant Managers** plan and supervise new plants, plant extensions, plant OT and equipment enhancement and modifications. Specifically, these individuals are responsible for people and operations at Solenis plants, warehouses, research facilities and other sites. Plant managers oversee security operations at their facilities and will coordinate with Executive teams in the establishment and administration of an OT Security Program.
- **OT supervisors,** at applicable sites, oversee the day-to-day activities of OT and security requirements of the plant.
- **Safety Engineers**, supervisors, or employees from the EHS (Environmental, Health and Safety) department would be tasked with monitoring, identifying, and communicating security risks regarding safety devices and their software to superior management.
- **Control System Engineers** and **DCS Administrators,** at applicable sites, manage the DCS, PCS, and OT systems locally at Solenis Plants. These engineers would be responsible for managing access to OT assets and ensuring that technically feasible controls and patches are applied to their assets.

4.0 Policy

All Solenis plants will establish, administer, and maintain an OT Security Program that provides a safe and secure workplace, and includes a reasonable level of protection for its employees, assets, processes, and information. An effective OT Security Program requires a balanced approach of employee commitment, operational procedures, security systems, and manual and technical controls to achieve an appropriate level of security without unnecessarily restricting or impeding regular business activities.

5.0 Guidelines and procedures / control

The purpose of this policy is to communicate the minimum required security controls to ensure the integrity, resiliency, and safety of Solenis plants. This policy initially applies to all systems within Solenis. Existing systems will be prioritized and then measured against this standard to develop action plans for remediation.

The structure of this OT Security Policy is aligned to the NIST Framework for Improving Critical Infrastructure Cybersecurity v.1.1, wherein overall cybersecurity activities are organized at their highest level to achieve the following key functions: Identify, Detect, Protect, Respond, and Recover.

5.1 Identify

5.1.1 Governance

- **Policies, procedures, standards and guidelines**
  - All OT Security Program policies, procedures, standards, and guidelines will be approved by management, published in an easily accessible location, and communicated to all stakeholders, OT asset owners, operators, and employees, as required in the performance of assigned duties.
  - An approved request for exemption from policy compliance must be formally obtained in circumstances where compliance to any OT security policy statements cannot be

achieved due to technical feasibility limitations, or when cost of compliance exceeds the benefit.
  - A review of the OT security policy guidelines will be performed annually, when significant changes to the systems occur, and as indicated by the results of security control assessments, to ensure the continued suitability, adequacy, and effectiveness of the security control requirements.
  - Management will require all employees and contractors to apply OT information security requirements in accordance with the established policies and procedures of Solenis.

Framework References: NIST CSF ID.GV-1; NIST 800-82 6.2.12, 6.2.18; IEC-62443 4.3.2.6.1-8

- **Roles and responsibilities**
  All information security and OT Security Program responsibilities pertaining to Solenis OT networks and locations will be appropriately identified and assigned.
  - Solenis Executive Team
    - Socialize and establish OT Security Policy control requirements
    - Manage and prioritize known risks emanating from the OT environment
    - Define risk characteristics per manufacturing site, to ensure risks are prioritized by business value of sites
  - Central Solenis Network Team
    - Identify any rogue OT assets in the corporate network
    - Validate that all manufacturing sites are protected by a firewall
    - Semi-annual review of OT firewall rules
  - Central Solenis Digital Security Team
    - Validate that endpoint security products and patches are available for local plant teams
    - Ensure that security logs from networks are aggregated in central SIEM
    - Provide support for investigation of security incident
  - Regional Infrastructure and Operations Teams
    - Work with local plant teams to install patches and endpoint security products
    - Collaborate with Central Solenis IT Security Team on any potential security alerts
    - Responsible for understanding Solenis Chain of Custody and Incident Response processes
  - Local Plant/Plant Teams (Plant Managers or their designee)
    - Capture and update asset management inventory and network architecture
    - Review OT Security Policy and request any necessary exceptions
    - Manage authorized electronic and physical access to OT systems

Framework References: NIST CSF ID.GV-2; NIST 800-82 6.2.13; IEC-62443 4.3.2.3.3

- **Identification of legislation and contractual requirements**
  All relevant legislative, statutory, regulatory, and contractual OT security requirements and Solenis' approach to meet these requirements will be explicitly identified, documented, and kept up to date for each Plant Site.
  Framework References: NIST CSF PR.IP-3, PR.MA-1, PR.MA-2; IEC-62443 4.3.4.3.2, 4.3.4.3.3, 4.3.3.3.7, 4.3.3.6.5-8

- **Intellectual property rights**
  Appropriate processes will be implemented to ensure compliance with legislative, regulatory, and contractual security requirements related to intellectual property rights and use of proprietary software products.

- **Change management**
  Plants should leverage Corporate IT processes for change management to ensure that all changes within plants are documented, tested, and approved prior to production release. OT system operators should leverage Corporate IT change management tools and records to audit any changes to OT applications.

  Framework References: NIST CSF ID.GV-3; NIST 800-82 6.2.17.2, 6.2.5;IEC-62443 4.4.3.7

5.1.2 Risk assessment

- **Threat identification**
  Both internal and external threats, associated with OT environments, will be identified and documented. Solenis Digital Security should disseminate threat intelligence information to plant sites, relevant to their industries, products, and technology stacks. Plant teams should ensure that Solenis Digital Security has an accurate inventory of currently deployed solutions and services.

  The threat impacts and likelihoods pertaining to OT environments will be identified and documented. Leveraging threat intelligence information gathered by Solenis Digital Security and known OT security risks.

  Framework References: NIST CSF ID.RA-2, ID.RA-3, ID.RA-5; NIST 800-82 6.2.14; IEC 62443 4.2.3.9, 4.2.3.12, 4.2.3.14, 4.2.3.10

- **Vulnerability identification**
  Hardware and software vulnerabilities present in Operating Technologies and applications leveraged in the plant environments should be identified and documented. Where technically feasible, leverage active or passive vulnerability scanning techniques. Deployment of vulnerability solutions should be prioritized based on the plant site risk level.

If vulnerability scanning is not technically feasible, accurate asset inventory data should be compared to publicly available vulnerability sources to identify potential vulnerabilities present.

Framework References: NIST CSF ID.RA-1, ID.RA-2, ID.RA-5, PR.IP-12, DE.CM-8, RS.AN-5, RS.MI-3; NIST 800-82 6.2.17.3, 6.2.4, 6.2.1.2; IEC 62443 4.2.3.3-5, 4.2.3.7, 4.2.3.7, 4.2.3.1

- **Determination of risk**
  Threats, vulnerabilities, impacts, and likelihood pertaining to OT environments will be used to determine the level of risk. Further, ESRM will develop a process to prioritize Solenis plants by their risk level to the organization – in High, Medium and Low Risk categories.

  Framework References: NIST CSF ID.GV-4, ID.RA-5, ID.RA-6; NIST 800-82 6.2.13, 6.2.14

5.1.3 Risk management strategy

- **Risk management process and risk tolerance**
  OT risk management processes will be established, managed, and agreed to by Solenis stakeholders. Solenis' OT risk tolerance will be determined based on leading industry indicators and externally available risk analyses, and formally communicated to appropriate stakeholders.

  Risk responses pertaining to OT environments will be identified and prioritized based upon their impact to Solenis' operations. Risk responses will be managed using one of the following options for each identified risk: Avoid, Mitigate, Transfer, Insure, or Accept. Risk responses will be documented within a plant site risk register and a centralized OT security risk register.

  Framework References: NIST CSF ID.RM-1, ID.RM-2, ID.RM-3; NIST 800-82 6.2.13, 6.2.14; IEC 62443 4.3.3.5.1, 4.3.2.6.5

- **Business impact analysis (BIA)**
  High-risk sites should conduct a business impact analysis across their business processes to identify critical applications / services and their dependencies. This information should inform disaster recovery and business continuity efforts.

  Framework References: NIST CSF ID.AM-5, ID.RA-4; NIST 800-82 6.2.6.1, 5.2; IEC 62443 4.2.3.6, 4.2.3.9, 4.2.3.11, 4.2.3.12

- **Supply Chain Risk Management**
  Solenis will regularly monitor, review and audit supplier service delivery and access to OT networks and assets. Solenis will enforce the Supplier Selection in Procurement Management Policy to assess third party suppliers, including cloud services.

Changes to the provision of services by OT suppliers, will be managed by an accountable Solenis employee, while considering the criticality of the information, systems and processes involved and potential reassessment of risks.
Agreements with suppliers will include requirements to address OT security risks associated with information and communications technology services and product supply chain. Plants should leverage existing process for third party risk management to identify and manage risks.

Framework References: NIST CSF ID.SC1-5, DE.CM-6; NIST 800-82 6.2.15; IEC-62443 4.2.3.1 - 4, 4.2.3.6, 4.2.3.8-10, 4.2.3.12-14

5.1.4 Asset management

- **Asset Inventory**
  Solenis hardware and software assets in the plant environments will be identified, and an inventory of these assets will be documented, maintained, and periodically reviewed. Initial inventories and associated configuration will be maintained within an enterprise provisioned application/database and periodically validated.

  The Asset Inventory should document, at a minimum, the following categories of assets and related metadata:

  - External Systems
    - Resource Priority
    - Data Classification Level
    - Remote Maintenance Channels
  - Software
    - Data Classification
    - System Scope
    - Versioning
    - System Criticality
    - Application dependencies
  - Hardware
    - Asset Name / Asset ID
    - Asset Category / Asset Type
    - Asset Owner
    - Resource Priority
    - Data Classification

  Framework References: NIST CSF ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4; NIST 800-82 6.2.15; IEC 62443 4.2.3.4

- **Asset management lifecycle**
  OT asset management processes for asset transfer and acceptable use should align with corporate IT processes for asset management. Where technically feasible, leverage

existing centrally managed technologies for efficiency gains and to ensure alignment of data quality and characteristics gathered.

All Solenis OT assets which contain, or have contained, sensitive information, and that is to be disposed of, will be destroyed by the most complete means possible, e.g., shredding, degaussing, or smashing.

Framework References: NIST CSF PR.DS-3; IEC 62443 4.3.3.3.9, 4.3.4.4.1

5.1.5 Business environment

- **Resiliency of system architecture**
  Plants should document network architecture diagrams and the associated data flows between assets on the plant network. Network architecture diagrams should be updated on at least a yearly basis. Overlay network architecture diagrams with asset priority, application dependencies, and capacity requirements to identify investment areas for resiliency of OT environments.

  Critical services and assets like network devices, control systems, and engineering workstations should have redundancy built in for high availability of services, hardware replacements available and support contracts or recovery procedures identified. On at least an annual basis plant IT teams should conduct capacity planning exercises to ensure proper alignment of IT resources to business operations.

  Framework References: NIST CSF ID.BE-5, PR.PT-5; IEC 62443 4.3.2.5.2

5.2 Protect

5.2.1 Access control

- **Least privilege**
  Users will only be provisioned access to OT network and network services that they have been specifically authorized to use (i.e., role-based privileges). Access to any network, endpoint and OT devices requires supervisor approval and documentation that includes rationale for access. Conflicting duties and areas of responsibility will be segregated to reduce opportunities for unauthorized or unintentional modification, or misuse of Solenis assets.

- **Provisioning and deprovisioning access**
  Where technically feasible, identities will be synced with corporate HR (Human Resources) systems to immediately revoke access for terminated individuals. Access will be revoked within 14 days on all applications and operating systems for accounts that cannot integrate with the Corporate HR systems.

  Framework References: NIST CSF PR.AC-4; NIST 800-82 6.2.1.1; IEC 62443 4.3.3.7.3

- **Remote access**
  Remote access to the OT network will be managed and restricted to only those Solenis personnel, contractors, and vendors with an approved operational need. Remote Access to plant networks may only utilize authorized remote access technologies provisioned by central Solenis. The maintenance and repair of OT hardware, firmware, and software via Remote Access should be performed in a timely manner, using approved and controlled tools. Remote Access should be restricted on a least privilege basis via Active Directory groups to Solenis employees and contractors with supervisor approval. Group membership should be restricted to only those sites necessary to access and should require Multi-Factor Authentication. Remote Access logs should be forwarded to the SIEM, and user access reviews conducted by plant leadership on at least a semi-annual basis.

  Framework References: NIST CSF PR.AC-3, PR.MA-2; NIST 800-82 5.15, 6.2.9, 6.2.1.2, 6.2.1.5, 6.2.1.4; IEC 62443 4.3.3.6.5-8

- **Privileged access management**
  Document all users that have access to group or shared accounts on engineering workstations, network devices, HMIs (human machine interfaces) or any other assets in plant environments. Where technically feasible, use complex passwords for group accounts that corporate Solenis standards, rotate passwords yearly or when a user with knowledge of the password is terminated or changes job roles (whichever comes first). Membership to group or shared accounts shall be reviewed on a semi-annual basis.

  Where technically feasible, privileged account secrets should be captured in a password vault or PAM solution provided by Corporate Solenis. Access attempts (successes and failures) to privileged secrets should be audited and forwarded to the corporate SIEM.

  Framework References: NIST CSF PR.AC-4, PR.AC-7, PR.AT-2; NIST 800-82 5.15, 6.2.1.1, 6.2.7.1; IEC 62443 4.3.3.7.3, 4.3.2.4.2, 4.3.2.4.3

- **Third-party access**
  All remote third-party access should be provisioned through existing Solenis account management process, with supervisor assignment and approval for remote access to provide maintenance. Account access shall be reviewed every 90 days and removed immediately if the contractor no longer requires access. Where technically feasible, restrict third party access to named accounts for named individuals. All third-party maintenance should be logged and monitored.

  If third party providers need to provide on-site maintenance, they shall be provided temporary accounts that are immediately disabled upon incident resolution and all third-party activity shall be monitored with a Solenis escort present.

  Framework References: NIST CSF PR.AC-3, PR.MA-2; NIST 800-82 5.15, 6.2.9, 6.2.1.2, 6.2.1.5, 6.2.1.4; IEC 62443 4.3.3.6.5-8

- **Password management**
  Where technically feasible, application and OS passwords should match Solenis password standards and accounts should be provisioned to named individuals. If password complexity is not feasible, at a minimum ensure length of password aligns with Solenis minimum password length requirements for IT systems. Where feasible, integrate identity solutions with HR processes to revoke access to terminated individuals in a timely manner.

  Default passwords used for system accounts will be renamed or disabled unless this is restricted by the vendor/supplier or is not technically feasible. This includes Administrator or Guest accounts.

  Framework References: NIST CSF PR.AC-1, PR.AC-6; NIST 800-82 6.2.7.1, 6.2.7.2; IEC 62443 4.3.3.5.1

5.2.2 Awareness and training

- **Information security awareness, education, and training**
  All employees and contractors of Solenis that access Solenis' OT / ICS assets will receive appropriate information security / OT Security Program awareness, education, and training in Solenis policies and procedures, which are relevant to their job function. OT-focused security awareness, education, and training will be provided upon hire, and at least annually thereafter.

  Additional OT training content will include understanding of the OT security roles and responsibilities for the following:
  - Privileged users
  - Third-party (e.g., suppliers, customers, contactors, and partners)
  - Senior executives
  - Physical and information security personnel

  Training records and metrics will be developed and reported periodically to the respective segment leads, to demonstrate effectiveness of OT security awareness, education, and training programs.

  Framework References: NIST CSF PR.AT-1, PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5; NIST 800-82 6.2.2, 6.2.6; IEC 62443 4.3.2.4.1-6

5.2.3 Malware protection

- **Endpoint security protection**
  Where technically feasible, endpoint security agents will be deployed to OT assets and security events forwarded to the Corporate SIEM.

  Large and medium-risk plants should consider endpoint detection / response (EDR) deployments with agents and signatures updated on release. Solenis Digital Security and

plant support personnel shall work collaboratively to respond to security alerts and maintain chain of custody procedures.

Smaller and medium-risk plants should implement whitelisting via endpoint protection, to restrict execution of software to only those specifically authorized. Whitelist inventory should be validated on at least a semi-annual basis and logs forwarded to the Corporate SIEM.

Where technically feasible, plants should collaborate with Solenis Digital Security to establish baseline images for Operating Systems in use. Legacy or unique operating systems may not have the capability to be hardened and other measures should be taken to increase monitoring of network traffic to the asset or restrict privileged access to the asset.

Framework References: NIST CSF DE.CM-4, DE.CM-5, DE.DP-1, RS.AN-1; NIST 800-82 6.2.17.1, 6.2.3, 6.2.11.2; IEC 62443 4.3.4.3.8, 4.4.3.1, 4.3.4.5.6-8

5.2.4 Physical security

- **Physical access**
  Physical access to OT assets will be managed and protected in accordance with a facility security plan. Where feasible, leverage badge access readers that are integrated with HR systems to revoke access in a timely manner to terminated employees or those with a job role change.

  At a minimum, Solenis facilities should have physical restrictions in place to prevent direct physical access to OT assets by unauthorized personnel. Where feasible, CCTV monitoring of access to sensitive areas and entry / exit points should be implemented with active monitoring of footage by physical security personnel. Additionally, Badge access readers integrated to HR systems should be deployed for entry / exit points and sensitive areas.

  Badge Access should be reviewed on at least a semi-annual basis to ensure appropriate access to facilities. Visitors should be escorted at all times and required to sign in prior to being granted access to facilities.

  Where it is not technically feasible to restrict access to OT systems by electronic means, physical security controls should be in place to prevent unauthorized access and CCTV in place to monitor physical access to devices.

  All OT assets and equipment must have at least one physical security control preventing direct access (ex: badge access, lock and key, biometric).

Vendor recommendations and industry stands for the physical operating environment of OT / ICS assets will be implemented at each Solenis facility to ensure temperature and humidity extremes, dust/dirt, and foreign object debris are mitigated to the extent possible.

Solenis facilities and areas that contain sensitive or critical electronic OT / ICS information will have defined electronic security perimeters that are housed within the demarcation of secured Solenis facilities. Any third-party facilities that act as an extension of Solenis operations and is connected to Solenis owned or leased OT systems will be included in the electronic perimeter.

Framework References: NIST CSF PR.AC-2, PR.AT-5, PR.IP-5, DE.CM-2; NIST 800-82 6.2.11, 6.2.16.1; IEC 62443 4.3.3.3.1-6, 4.3.3.3.8, 4.3.2.4.2

5.2.5 Portable media

- **Removable media**

  The use of any removable media or storage devices (e.g. USB drives, CD/DVD) on OT / ICS assets will only be permitted where no reasonable alternative exists and only when authorized by the designated asset owner. Corporate Solenis will provide assistance in deploying technical controls to prevent USB usage and monitoring capabilities to ensure authorized USB devices do not carry malware.

  Framework References: NIST CSF PR.PT-2; NIST 800-82 6.2.11.2, 6.2.17.1

5.2.6 Network protection

- **Network controls**

  OT networks should be segmented from Corporate Solenis via a corporate provisioned firewall. OT sites should not have direct connectivity to one another, without prior authorization from ESRM. The OT network firewall should forward logs to the corporate SIEM, have access restricted and reviewed on a quarterly basis, be patched on at least a semi-annual basis or as needed to maintain 'n - 1' version and its firewall rules should be validated on at least a semi-annual basis. Change auditing should be enabled to identify any firewall rule changes and a change record should be submitted with Solenis ESRM approval for any firewall rule changes.

  Direct Internet access from the plant floors increases the risk to plant assets significantly and should be restricted unless absolutely necessary for plant operations. Steps should be taken to gain approval from ESRM, and document Internet access needed.

  Privileged access to switches and routers within the OT networks should be restricted and reviewed for appropriate access on at least a quarterly basis. Group and shared logins should be stored within an authorized Privileged Access Management solution (see section 6.2.1) and meet Solenis corporate standards for password management. Where technically feasible, network logs should be captured and able to be shared with Solenis Digital Security in the event of a security incident.

High-risk and medium-risk facilities should implement OT security products to passive gather additional visibility into OT networks and expected traffic flows.

Wireless networks with connectivity to control systems / ICS should not be utilized unless explicitly approved by ESRM. If wireless capabilities are needed, ensure that access to access points is restricted, patches are applied on a monthly basis, access attempts to management ports are logged, and passwords are rotated on a monthly basis and meet Corporate Solenis password management standards. Visitor wireless networks within the plant environment should be avoided. IP enabled devices will not be dual-homed with IP addresses provisioned to plant networks and corporate networks.

OT development and testing environments will be separated from OT production environments. Testing of OT security functionality will be carried out during development or for newly acquired systems.

Framework References: NIST CSF PR.AC-5, PR.PT-4, DE.AE-1, DE.CM-1; NIST 800-82 5.15, 6.2.1.5, 5.1, 5.2, 5.3, 6.2.11.3, 6.2.17.2, 6.2.5, 5.6, 5.7, 5.8.1, 5.8.7-10, 5.9, 5.11, 5.5.1; IEC 62443 4.4.3.3, 4.3.3.4.1-3

5.2.7 Patch management

- **Patch management**
  Where technically feasible, OT systems should review lists of available patches and rank these in order of criticality (critical / high / medium / low) based on CVSS score or vendor recommendation. Patches, hotfixes, or updates addressing security vulnerabilities with proof-of-concept should be treated as Critical. Critical patches should be applied on a monthly basis, high-risk patches on a quarterly basis and all other patches on an as needed basis. If OS (Operating Systems) or applications are legacy and patches are no longer available, ensure additional mitigating controls are in place and privileged access is restricted.

  Where technically feasible, information on patch priority and associated risk of missing patch shall come from authorized vulnerability management solutions. If those solutions are unavailable to the plant, query critical systems locally to determine their patch levels and consult Solenis Digital Security team on how to prioritize patching efforts.

  Proper testing and preparation for patching OT systems is required. Where available, test patches in testing and development environments first. Plant teams should work with vendors and Solenis Digital Security team for any questions about how to apply patches or the potential impacts to OT assets from applying patches.

  Framework References: NIST CSF ID.RA-1, ID.RA-2, ID.RA-5, PR.IP-12, DE.CM-8, RS.AN-5, RS.MI-3; NIST 800-82 6.2.17.3, 6.2.11.2, 6.2.17.1, 6.2.3; IEC 62443 4.2.3.3-5, 4.2.3.7, 4.2.3.7, 4.2.3.1

5.2.8 Safety systems protection

- **Safety systems**
  Laptops which are required for configuring safety systems must be dedicated laptops which are used exclusively for this purpose. Safety systems will be separated from the control network by a network device (firewall or router) that only permits traffic required for the safety systems to operate. This can be established with firewall rules or router ACLs (Access Control Lists). Industrial components and instrumentation that are part of a safety system or capable of changing parameters of a safety system will not be remotely user accessible from any network, including network segments in the same industrial network.

5.3 Detect

5.3.1 Logging and monitoring

- **Event logs**
  Event logs recording user activities, exceptions, faults, and OT / ICS security events will be produced, retained, and regularly reviewed. Event Logs will contain at minimum following aspects related to the occurrence:
  - User identification
  - Type of event
  - Date and time
  - Source or origination of event
  - Success or Failure indication, where applicable

  All sites should forward firewall logs (failed connection attempt), remote access logs (success and failed logins) and available endpoint protection logs (security alerts) to the Corporate SIEM. Solenis Digital Security will assist in any technical guidance needed.

  Facilities should additionally capture logs on local systems for changes to firewall rules, OT system configuration changes, badge access attempts, and host OS logs. Access to logs should be restricted and access to logs reviewed on a quarterly basis.

  Reliable time synchronization technologies (e.g. NTP) will be utilized for each plant to ensure integrity of event logs.

  Framework References: NIST CSF PR.PT-1, DE.AE-2-4, DE.CM-1-7, DE.DP-1-5; NIST 800-82 6.2.17, 6.2.8, 6.2.3, 6.2.11, 5.16; IEC 62443 4.3.3.3.8-9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1-2, 4.4.2.4, 4.3.4.5.6-9, 4.4.3.1-2, 4.4.3.4

5.4 Respond

5.4.1 Incident response

- **Incident response**
  Plant Managers, Plant Site Operators and personnel using Solenis' OT assets will be required to note and report any observed or suspected information security weaknesses in systems or services to Solenis Digital Security. Technical staff at plant sites should be trained of chain of custody procedures and the appropriate channels to communicate OT security incident information to Solenis Digital Security.

Solenis Digital Security shall develop and maintain OT security incident response playbooks for OT environments and share with technical leads for plant sites. High- and medium-risk sites should conduct cybersecurity tabletop exercises once every 18 months. Lower-risk sites should conduct cybersecurity tabletop exercises once every 24 to 36 months.

On-site plant personnel should contact Solenis Digital Security if they suspect there is a security incident in their environment. On-site personnel should be prepared to grant privileged access to Corporate Solenis Digital Security or provide logs to aid in incident response activities.

Plant managers should be involved early and often in incident response activities and must provide written approval for removing critical OT systems from production to contain malware. Incident response activities should follow Solenis Digital Security standards for incident response.

Framework References: NIST CSF PR.IP-9, PR.IP-10, DE.AE-5, DE.DP-1, RS.RP-1, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.AN-1, RS.AN-2, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2; NIST 800-82 6.2.8, 6.2.6; IEC 62443 4.3.2.5.3, 4.3.4.5.1-8, 4.3.2.5.7, 4.3.4.5.11, 4.4.3.1, 4.3.4.5.10, 4.4.3.4

5.5 Recover

5.5.1 Business continuity and disaster recovery

- **Business continuity**

  On-site plant teams will establish, document, implement and maintain processes, procedures, and controls to ensure the required level of continuity for plant operations during an adverse situation. Corporate Solenis will provide template and training guides to meet standards. Plant teams will verify the established and implemented OT continuity controls on an annual basis via tabletop exercises in order to ensure that they are valid and effective during adverse situations. Business continuity plans should include call trees, procedures for maintaining plant operations, escalation procedures, stakeholders to involve, communications template and engagement with Public Relations. Where necessary, integrate Continuity Plans with Health and Safety Response Procedures.

  Framework References: NIST CSF ID.AM-5, ID.RA-4, PR.IP-9; NIST 800-82 6.2.6; IEC 62443 4.3.2.5.3, 4.3.4.5.1, 4.2.3.6, 4.2.3.9, 4.2.3.11, 4.2.3.12

- **Disaster recovery (DR)**

  Solenis plants should identify applications and services critical to plant operations. These critical services / applications should have defined recovery procedures, Recovery Time Objectives (RTO’s), Recovery Point Objectives (RPOs) and primary point of contact identified. High and Medium-risk facilities should conduct DR tests every 18 months. Low-risk facilities should conduct DR tests every 36 months. Corporate Solenis will provide templates and training on building DR plans.

Framework References: NIST CSF ID.SC-5, PR.IP-9, PR.IP-10, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-3; NIST 800-82 6.2.6, 6.2.6.1, 6.2.6.2; IEC 62443 4.3.2.5.3, 4.3.4.5.1, 4.3.2.5.7, 4.3.4.5.11, 4.4.3.4

- **Backup and recovery**
  Solenis plants at a minimum should backup on a monthly basis – data for critical applications, configurations for OT assets, and configurations for network devices. Where technically feasible, leverage data backup technologies from Corporate Solenis and replicate backups onto a separate location than the asset the backup data was gathered from. Access to backup software and data should be restricted and reviewed on at least a semi-annual basis.

  Higher-risk plants should leverage immutable backups where possible, test backup restores on a quarterly basis and backup VM images for critical application servers and workstations.

  Framework References: NIST CSF PR.IP-4; NIST 800-82 6.2.6.2, 5.7, 6.2.11; IEC 62443 4.3.4.3.9

6.0 Definitions

Physical Access Control – A program comprised of security equipment and procedural controls to limit building access to authorized persons only.

Electronic Access Control System – An electronic system that restricts access to Solenis sites or areas to authorized persons by using some form of pre-programmed credentials, electronic locks, magnetic door position switches, readers, control panels and servers.

Plant Site – Manufacturing location owned by Solenis, or its subsidiaries, that manufactures products for Solenis.

Operational Technology (OT) – software and hardware technologies used to control and monitor the tasks performed by operation tools and processes, network devices, and plant equipment.

Supervisory control and data acquisition (SCADA) – This is a combination of software and hardware elements that control industrial systems or processes located locally or globally. The systems are widely used in water treatment and distribution plants across the world. These plants have a specific set of software to view, monitor, and control the control systems hardware by using the network interface. Based on data gathered from multiple control systems globally, managers or supervisors would take steps to control outputs.

Distributed Control Systems (DCS) – DCS is a system of sensors, controllers, and computer systems that are distributed throughout the plant. Based on the operations, automatic adjustments are made to have a continuous flow of operations.

Program Logic Controllers (PLCs) – These are digital systems that have programmed instructions to carry out operations from one point to another point.

Industrial Control Systems (ICS) – General term that encompasses several types of control systems, including SCADA systems, DCS, and other control system configurations such as PLCs often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, etc.) that act together to achieve an industrial objective.

Human-Machine Interface (HMI) – The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.

OT Database – This is a centralized database that logs all information related to control systems globally. The logged information is used as a reference for security monitoring activity, capacity planning, events that occurred, and access related activity.

IO Servers – IO servers collect and store the information required for operating operational technology and equipment.

Security information and event management (SIEM) – Technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events.

RTO (Recovery Time Objective) – Time required to recover the required communication links and processing capabilities

RPO (Recovery Point Objective) – Recovery of data describing production (SCADA) in the past and is usually specified time

7.0 References

- SL-POL-006.005 Information Security Standards
- SL-PRO-005.075 Physical Security Procedure
- SL-POL-008.006 Procurement of Goods and Services
- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Draft version 1.1 – I.E. NIST CSF
- National Institute of Standards and Technology (NIST) Special Publication 800-82 – Guide to Industrial Control Systems (ICS) Security
- IECEE Industrial Cyber Security Program 62443

8.0 Owner

Director, Digital Security

9.0 Exceptions

There are no exceptions to this policy.