



Omella Data Security and Privacy Plan

Policy Statement

This document explains Omella's Information Security Management System (ISMS) and information security (infosec) governance efforts within the organization that are relevant to the state, federal, and local data security and privacy contract requirements set forth by the New York Department of Education for subcontractors. Omella will maintain and review this Data Security and Privacy Plan, no less than annually, with the objective of demonstrating the approach for ongoing compliance with these requirements.

Scope

This policy applies to all Omella employees, contractors, and third parties ("users") using its electronic resources, and is part of the Omella corporate information security policy to support active agreements with organizations and educational institutions in the state of New York.

Personnel Training

Omella is required by regulation and law to protect the personally identifiable information and personal data of all of our users no matter their ages. Omella requires employees to receive privacy training at the time of hire and on a regular basis thereafter, no less than annually, to ensure their understanding of the relevant regulations and laws that Omella must comply with. These laws include:

- Various US states' student privacy laws including, without limitation, New York State Education Law § 2-d ("New York Ed. 2-d), and Section 121 of New York regulations that implement that law and related law.
- The Family Educational Rights Privacy Act (FERPA);
- The Children's Online Privacy Protection Act (COPPA); and,
- European Union General Data Protection Regulation.

Supplier Management

Supplier management practices must be consistent with Omella's Vendor Risk Management Policy, including the following key activities.

New Vendors

Prior to engaging any new vendors or suppliers, Omella reviews their security and privacy to determine whether the vendor or supplier practices satisfy our standards and our legal and contractual commitments. Once the vendor has been categorized based on the nature of the service, a review of the vendor's security relative to the corresponding risk tier is to be done prior to sharing any Omella or customer data with the vendor.

Omella requires that contractual terms with new vendors must include, at a minimum, requisite data protection requirements and the return or destruction of all Omella data upon termination of vendor services consistent with language contained in the Omella Data Processing Addendum.

Vendor Oversight and Monitoring

A risk-based approach is taken for vendor security oversight, where more rigor and in-depth analysis are applied to vendors with whom sensitive data is exchanged. All vendors are subject to an annual review of security, but different focus and scrutiny are directed to different vendor tiers.

Terminating Vendor Relationships

Upon termination, procurement and operations personnel are to immediately ensure active data transfers of Omella data cease, and access to Omella information systems is revoked.

Information Security Incident Management

The handling of information security incidents will be consistent with Omella's confidential Security Incident Response Plan, including processes to support:

- Detection of security incidents
- Classification of security incidents
- Steps to verify, contain, investigate, mitigate and recover
- Incident report documentation
- Any additional technical or procedural efforts required to prevent a subsequent incident

Legal Compliance

Consistent with Omella's corporate security policy, and other applicable laws and regulations, the vendor or supplier may be required to notify regulatory and law enforcement agencies, as well as its customers, of incidents involving unauthorized access to or use of customer or employee information, etc. Omella shall comply with all notice requirements under the security guidelines. Omella's legal department will consult with other representatives, as necessary, to determine whether, and which agencies must receive notice, as well as the manner, content, and timing of delivery of such notices, based on certain standards. To the extent necessary, Omella may elect to consult with internal and external counsel.

The requirement should include but are not limited to the following parties (if applicable):

- Regulatory agencies
- Law enforcement
- Federal Bureau of Investigation
- Local police department
- Customers
- Omella users
- Service providers or third parties (if any)

Depending on the nature of the threat and assessed risk, "Standards" for providing notice(s) as a whole or just to those impacted may be used (limited notices)

Data Retention and Destruction

Omella will either delete or return, within a commercially reasonable period of time but not to

exceed 45 days, all personally identifiable information upon the expiration of any agreement when requested to do so in writing by notification, as that term is defined in Omella's contract with the contracting party, from the contracting party.

General Controls

Omella has adopted ISO/IEC 27001 and ISO/IEC 27002 as a framework for the design and monitoring of administrative, operational, and technical safeguards to maintain integrity, availability, and confidentiality of personally identifiable information.

To demonstrate how Omella's ISMS is consistent with the NIST Cybersecurity Framework V1.1, a bridge mapping for the control is defined as follows.

Category	Subcategory	Informative References
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	· CCS CSC 1
		· COBIT 5 BAI09.01, BAI09.02
		· ISA 62443-2-1:2009 4.2.3.4
		· ISA 62443-3-3:2013 SR 7.8
		· ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
		· NIST SP 800-53 Rev. 4 CM-8
	ID.AM-2: Software platforms and applications within the organization are inventoried	· CCS CSC 2
		· COBIT 5 BAI09.01, BAI09.02, BAI09.05
		· ISA 62443-2-1:2009 4.2.3.4
		· ISA 62443-3-3:2013 SR 7.8
		· ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
		· NIST SP 800-53 Rev. 4 CM-8
	ID.AM-3: Organizational communication and data flows are mapped	· CCS CSC 1

		· COBIT 5 DSS05.02
		· ISA 62443-2-1:2009 4.2.3.4
		· ISO/IEC 27001:2013 A.13.2.1
		· NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
	ID.AM-4: External information systems are catalogued	· COBIT 5 APO02.02
		· ISO/IEC 27001:2013 A.11.2.6
		· NIST SP 800-53 Rev. 4 AC-20, SA-9
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· COBIT 5 APO03.03, APO03.04, BAI09.02
		· ISA 62443-2-1:2009 4.2.3.6
		· ISO/IEC 27001:2013 A.8.2.1
		· NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· COBIT 5 APO01.02, DSS06.03
		· ISA 62443-2-1:2009 4.3.2.3.3
		· ISO/IEC 27001:2013 A.6.1.1
		· NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated	· COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05
		· ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2
		· NIST SP 800-53 Rev. 4 CP-2, SA-12
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is	· COBIT 5 APO02.06, APO03.01
		· NIST SP 800-53 Rev. 4 PM-8

	identified and communicated	
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· COBIT 5 APO02.01, APO02.06, APO03.01
		· ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6
		· NIST SP 800-53 Rev. 4 PM-11, SA-14
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3
		· NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
	ID.BE-5: Resilience requirements to support delivery of critical services are established	· COBIT 5 DSS04.02
		· ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1
		· NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established	· COBIT 5 APO01.03, EDM01.01, EDM01.02
		· ISA 62443-2-1:2009 4.3.2.6
		· ISO/IEC 27001:2013 A.5.1.1
		· NIST SP 800-53 Rev. 4 -1 controls from all families
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	· COBIT 5 APO13.12
		· ISA 62443-2-1:2009 4.3.2.3.3
		· ISO/IEC 27001:2013 A.6.1.1, A.7.2.1
		· NIST SP 800-53 Rev. 4 PM-1, PS-7
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are	· COBIT 5 MEA03.01, MEA03.04
		· ISA 62443-2-1:2009 4.4.3.7

	understood and managed	· ISO/IEC 27001:2013 A.18.1
		· NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
	ID.GV-4: Governance and risk management processes address cybersecurity risks	· COBIT 5 DSS04.02
		· ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3
		· NIST SP 800-53 Rev. 4 PM-9, PM-11
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	· CCS CSC 4
		· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04
		· ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12
		· ISO/IEC 27001:2013 A.12.6.1, A.18.2.3
		· NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	· ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12
		· ISO/IEC 27001:2013 A.6.1.4
		· NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5
	ID.RA-3: Threats, both internal and external, are identified and documented	· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04
		· ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12
		· NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
	ID.RA-4: Potential business impacts and likelihoods are identified	· COBIT 5 DSS04.02
		· ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12

		· NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· COBIT 5 APO12.02
		· ISO/IEC 27001:2013 A.12.6.1
		· NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RA-6: Risk responses are identified and prioritized	· COBIT 5 APO12.05, APO13.02
		· NIST SP 800-53 Rev. 4 PM-4, PM-9
	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	· COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02
		· ISA 62443-2-1:2009 4.3.4.2
		· NIST SP 800-53 Rev. 4 PM-9
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· COBIT 5 APO12.06
		· ISA 62443-2-1:2009 4.3.2.6.5
		· NIST SP 800-53 Rev. 4 PM-9
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	· NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14
Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users	· CCS CSC 16
		· COBIT 5 DSS05.04, DSS06.03
		· ISA 62443-2-1:2009 4.3.3.5.1
		· ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
		· ISO/IEC 27001:2013 A.9.2.1, A.9.2.2,

		A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
		· NIST SP 800-53 Rev. 4 AC-2, IA Family
	PR.AC-2: Physical access to assets is managed and protected	· COBIT 5 DSS01.04, DSS05.05
		· ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8
		· ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3
		· NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
	PR.AC-3: Remote access is managed	· COBIT 5 APO13.01, DSS01.04, DSS05.03
		· ISA 62443-2-1:2009 4.3.3.6.6
		· ISA 62443-3-3:2013 SR 1.13, SR 2.6
		· ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1
		· NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	· CCS CSC 12, 15
		· ISA 62443-2-1:2009 4.3.3.7.3
		· ISA 62443-3-3:2013 SR 2.1
		· ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
		· NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16
	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	· ISA 62443-2-1:2009 4.3.3.4
		· ISA 62443-3-3:2013 SR 3.1, SR 3.8
		· ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1

		· NIST SP 800-53 Rev. 4 AC-4, SC-7
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained	· CCS CSC 9
		· COBIT 5 APO07.03, BAI05.07
		· ISA 62443-2-1:2009 4.3.2.4.2
		· ISO/IEC 27001:2013 A.7.2.2
		· NIST SP 800-53 Rev. 4 AT-2, PM-13
	PR.AT-2: Privileged users understand roles & responsibilities	· CCS CSC 9
		· COBIT 5 APO07.02, DSS06.03
		· ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3
		· ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
		· NIST SP 800-53 Rev. 4 AT-3, PM-13
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	· CCS CSC 9
		· COBIT 5 APO07.03, APO10.04, APO10.05
		· ISA 62443-2-1:2009 4.3.2.4.2
		· ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
		· NIST SP 800-53 Rev. 4 PS-7, SA-9
	PR.AT-4: Senior executives understand roles & responsibilities	· CCS CSC 9
		· COBIT 5 APO07.03
		· ISA 62443-2-1:2009 4.3.2.4.2
		· ISO/IEC 27001:2013 A.6.1.1, A.7.2.2,
		· NIST SP 800-53 Rev. 4 AT-3, PM-13

		· CCS CSC 9
	PR.AT-5: Physical and information security personnel understand roles & responsibilities	· COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.		· CCS CSC 17
	PR.DS-1: Data-at-rest is protected	· COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 · ISA 62443-3-3:2013 SR 3.4, SR 4.1 · ISO/IEC 27001:2013 A.8.2.3 · NIST SP 800-53 Rev. 4 SC-28
		· CCS CSC 17
	PR.DS-2: Data-in-transit is protected	· COBIT 5 APO01.06, DSS06.06 · ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SC-8
		· COBIT 5 BAI09.03
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7

		· NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
	PR.DS-4: Adequate capacity to ensure availability is maintained	· COBIT 5 APO13.01
		· ISA 62443-3-3:2013 SR 7.1, SR 7.2
		· ISO/IEC 27001:2013 A.12.3.1
		· NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
	PR.DS-5: Protections against data leaks are implemented	· CCS CSC 17
		· COBIT 5 APO01.06
		· ISA 62443-3-3:2013 SR 5.2
		· ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
		· NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8
		· ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
		· NIST SP 800-53 Rev. 4 SI-7
	PR.DS-7: The development and testing environment(s) are separate from the production environment	· COBIT 5 BAI07.04
		· ISO/IEC 27001:2013 A.12.1.4
		· NIST SP 800-53 Rev. 4 CM-2
Information Protection Processes and Procedures (PR.IP): Security policies	PR.IP-1: A baseline configuration of information technology/industrial control	· CCS CSC 3, 10
		· COBIT 5 BAI10.01, BAI10.02, BAI10.03,

(that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	systems is created and maintained	BAI10.05
		· ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3
		· ISA 62443-3-3:2013 SR 7.6
		· ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
		· NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	· COBIT 5 APO13.01
		· ISA 62443-2-1:2009 4.3.4.3.3
		· ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5
		· NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
	PR.IP-3: Configuration change control processes are in place	· COBIT 5 BAI06.01, BAI01.06
		· ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3
		· ISA 62443-3-3:2013 SR 7.6
		· ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
		· NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	· COBIT 5 APO13.01
		· ISA 62443-2-1:2009 4.3.4.3.9
		· ISA 62443-3-3:2013 SR 7.3, SR 7.4
		· ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3
		· NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9

	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	· COBIT 5 DSS01.04, DSS05.05
		· ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6
		· ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
		· NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
	PR.IP-6: Data is destroyed according to policy	· COBIT 5 BAI09.03
		· ISA 62443-2-1:2009 4.3.4.4.4
		· ISA 62443-3-3:2013 SR 4.2
		· ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
		· NIST SP 800-53 Rev. 4 MP-6
	PR.IP-7: Protection processes are continuously improved	· COBIT 5 APO11.06, DSS04.05
		· ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8
		· NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	· ISO/IEC 27001:2013 A.16.1.6
		· NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· COBIT 5 DSS04.03
		· ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1
		· ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2
		· NIST SP 800-53 Rev. 4 CP-2, IR-8

	PR.IP-10: Response and recovery plans are tested	· ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11
		· ISA 62443-3-3:2013 SR 3.3
		· ISO/IEC 27001:2013 A.17.1.3
		· NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
		· ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3
		· ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4
		· NIST SP 800-53 Rev. 4 PS Family
	PR.IP-12: A vulnerability management plan is developed and implemented	· ISO/IEC 27001:2013 A.12.6.1, A.18.2.2
		· NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	· COBIT 5 BAI09.03
		· ISA 62443-2-1:2009 4.3.3.3.7
		· ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5
		· NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	· COBIT 5 DSS05.04
		· ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8
		· ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1
		· NIST SP 800-53 Rev. 4 MA-4

Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· CCS CSC 14
		· COBIT 5 APO11.04
		· ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4
		· ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
		· ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
	PR.PT-2: Removable media is protected and its use restricted according to policy	· NIST SP 800-53 Rev. 4 AU Family
		· COBIT 5 DSS05.02, APO13.01
		· ISA 62443-3-3:2013 SR 2.3
		· ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9
		· NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	· COBIT 5 DSS05.02
		· ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4
		· ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
		· ISO/IEC 27001:2013 A.9.1.2
		· NIST SP 800-53 Rev. 4 AC-3, CM-7

	PR.PT-4: Communications and control networks are protected	· CCS CSC 7
		· COBIT 5 DSS05.02, APO13.01
		· ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6
		· ISO/IEC 27001:2013 A.13.1.1, A.13.2.1
		· NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	· COBIT 5 DSS03.01
		· ISA 62443-2-1:2009 4.4.3.3
		· NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
		· ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
		· ISO/IEC 27001:2013 A.16.1.1, A.16.1.4
		· NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	· ISA 62443-3-3:2013 SR 6.1
		· NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
	DE.AE-4: Impact of events is determined	· COBIT 5 APO12.06
		· NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
	DE.AE-5: Incident alert thresholds are established	· COBIT 5 APO12.06

Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.		· ISA 62443-2-1:2009 4.2.3.10
		· NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
	DE.CM-1: The network is monitored to detect potential cybersecurity events	· CCS CSC 14, 16
		· COBIT 5 DSS05.07
		· ISA 62443-3-3:2013 SR 6.2
		· NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	· ISA 62443-2-1:2009 4.3.3.3.8
		· NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	· ISA 62443-3-3:2013 SR 6.2
		· ISO/IEC 27001:2013 A.12.4.1
		· NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
	DE.CM-4: Malicious code is detected	· CCS CSC 5
		· COBIT 5 DSS05.01
		· ISA 62443-2-1:2009 4.3.4.3.8
		· ISA 62443-3-3:2013 SR 3.2
		· ISO/IEC 27001:2013 A.12.2.1
	DE.CM-5: Unauthorized mobile code is detected	· NIST SP 800-53 Rev. 4 SI-3
		· ISA 62443-3-3:2013 SR 2.4
		· ISO/IEC 27001:2013 A.12.5.1
		· NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44

	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· COBIT 5 APO07.06
		· ISO/IEC 27001:2013 A.14.2.7, A.15.2.1
		· NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
	DE.CM-8: Vulnerability scans are performed	· COBIT 5 BAI03.10
		· ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7
		· ISO/IEC 27001:2013 A.12.6.1
		· NIST SP 800-53 Rev. 4 RA-5
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	· CCS CSC 5
		· COBIT 5 DSS05.01
		· ISA 62443-2-1:2009 4.4.3.1
		· ISO/IEC 27001:2013 A.6.1.1
		· NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
	DE.DP-2: Detection activities comply with all applicable requirements	· ISA 62443-2-1:2009 4.4.3.2
		· ISO/IEC 27001:2013 A.18.1.4
		· NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4
	DE.DP-3: Detection processes are tested	· COBIT 5 APO13.02
		· ISA 62443-2-1:2009 4.4.3.2
		· ISA 62443-3-3:2013 SR 3.3

		· ISO/IEC 27001:2013 A.14.2.8
		· NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
	DE.DP-4: Event detection information is communicated to appropriate parties	· COBIT 5 APO12.06
		· ISA 62443-2-1:2009 4.3.4.5.9
		· ISA 62443-3-3:2013 SR 6.1
		· ISO/IEC 27001:2013 A.16.1.2
		· NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4
	DE.DP-5: Detection processes are continuously improved	· COBIT 5 APO11.06, DSS04.05
		· ISA 62443-2-1:2009 4.4.3.4
		· ISO/IEC 27001:2013 A.16.1.6
		· NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event	· COBIT 5 BAI01.10
		· CCS CSC 18
		· ISA 62443-2-1:2009 4.3.4.5.1
		· ISO/IEC 27001:2013 A.16.1.5
		· NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies	RS.CO-1: Personnel know their roles and order of operations when a response is needed	· ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4
		· ISO/IEC 27001:2013 A.6.1.1, A.16.1.1
		· NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8

	RS.CO-2: Events are reported consistent with established criteria	· ISA 62443-2-1:2009 4.3.4.5.5
		· ISO/IEC 27001:2013 A.6.1.3, A.16.1.2
		· NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
	RS.CO-3: Information is shared consistent with response plans	· ISA 62443-2-1:2009 4.3.4.5.2
		· ISO/IEC 27001:2013 A.16.1.2
		· NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· ISA 62443-2-1:2009 4.3.4.5.5
		· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· NIST SP 800-53 Rev. 4 PM-15, SI-5
	RS.AN-1: Notifications from detection systems are investigated	· COBIT 5 DSS02.07
		· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
		· ISA 62443-3-3:2013 SR 6.1
		· ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5
		· NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
	RS.AN-2: The impact of the incident is understood	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
		· ISO/IEC 27001:2013 A.16.1.6
		· NIST SP 800-53 Rev. 4 CP-2, IR-4

	RS.AN-3: Forensics are performed	· ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
		· ISO/IEC 27001:2013 A.16.1.7
		· NIST SP 800-53 Rev. 4 AU-7, IR-4
	RS.AN-4: Incidents are categorized consistent with response plans	· ISA 62443-2-1:2009 4.3.4.5.6
		· ISO/IEC 27001:2013 A.16.1.4
		· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-1: Incidents are contained	· ISA 62443-2-1:2009 4.3.4.5.6
		· ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4
		· ISO/IEC 27001:2013 A.16.1.5
		· NIST SP 800-53 Rev. 4 IR-4
	RS.MI-2: Incidents are mitigated	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10
		· ISO/IEC 27001:2013 A.12.2.1, A.16.1.5
		· NIST SP 800-53 Rev. 4 IR-4
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	· ISO/IEC 27001:2013 A.12.6.1
		· NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	· COBIT 5 BAI01.13
		· ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4
		· ISO/IEC 27001:2013 A.16.1.6
		· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	RS.IM-2: Response strategies	· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

	are updated	
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	· CCS CSC 8
		· COBIT 5 DSS02.05, DSS03.04
		· ISO/IEC 27001:2013 A.16.1.5
		· NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	· COBIT 5 BAI05.07
		· ISA 62443-2-1 4.4.3.4
		· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	RC.IM-2: Recovery strategies are updated	· COBIT 5 BAI07.08 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed	· COBIT 5 EDM03.02
	RC.CO-2: Reputation after an event is repaired	· COBIT 5 MEA03.02
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	· NIST SP 800-53 Rev. 4 CP-2, IR-4