PSO

PRODUCE SUPPLY.ORG

PSOCSC (PSO Cybersecurity Council) Implementation Core

Wednesday, July 13, 2022

KEY OBJECTIVES

Make produce industry suppliers safer from cyber-attack by:

1) Developing a culture of transparency and shared communication amongst members and non-members.
2) Defining a lightweight framework, based on the NIST Cybersecurity Framework that is specifically applicable to produce industry suppliers.
3) Creating a **set of actionable best practices** categorized and based on the above framework.
4) Building an outreach plan to market and distribute the set of best practices to produce suppliers.
5) Continuously improve on the best practices by using real world learnings and measured control monitoring.

PSO
PRODUCE SUPPLY.ORG

FRAMEWORK CORE FUNCTIONS

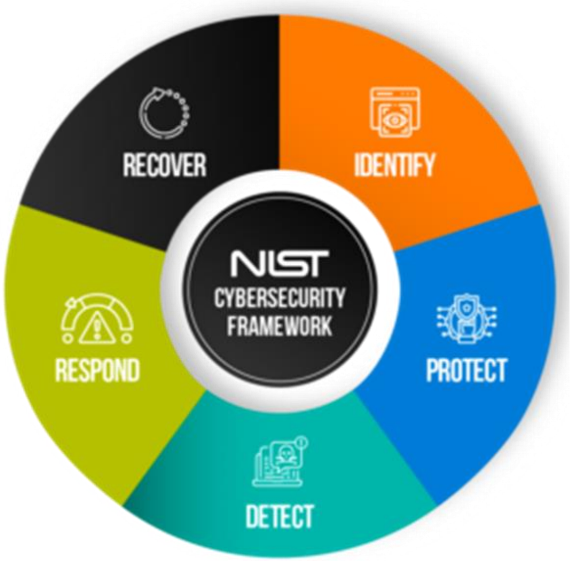
Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Protect – Develop and implement appropriate safeguards to ensure delivery of critical services.

Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.



PSO
PRODUCE SUPPLY.ORG

NIST Framework for Improving Critical Infrastructure Cybersecurity

A Tool to Help Identify and Prioritize Actions for Reducing Cybersecurity Risk

IDENTIFY

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management

PROTECT

- Identify Management and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes & Procedures
- Maintenance
- Protective Technology

DETECT

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

RESPOND

- Response Planning
- Communications (IR)
- Analysis
- Mitigation
- Improvements

RECOVER

- Recovery Planning
- Improvements
- Communications (DR)

PSO Cybersecurity Standards – Identify (1 / 4)

	High Tier	Middle Tier	Low Tier
ID.AM-1: Physical devices and systems are inventoried	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets via automated processes with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers.	Document an inventory of production system components (including portable) that reflects the current system.	Document an inventory of production system components that reflects the current system.
	Implement automated mechanisms for detecting the presence of unauthorized hardware and firmware components	Identify mechanisms (via software and/or policy) for detecting the presence of unauthorized hardware and firmware components	
	Establish and maintain architecture diagram(s) and/or other network system documentation. Employ automated processes where possible.	Establish and maintain architecture diagram(s) and/or other network system documentation.	
ID.AM-2: Software platforms and applications are inventoried	Document an inventory of software and firmware components within the enterprise.	Document an inventory of software and firmware components within the enterprise.	Document an inventory of software and firmware components within the enterprise.
	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets.	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets.	
ID.AM-4: External information systems are catalogued	Require external providers to identify the functions, ports, protocols, and other services required for external vendors to access the enterprise's networks, maintain these records current.	Discuss and document external provider access mechanisms into the enterprise's networks.	Discuss and document external provider access mechanisms into the enterprise's networks.
	Identify and catalog all cloud providers utilized by the enterprise and the interface mechanisms employed (APIs, portals, etc.). Maintain these records current.	Identify and catalog all cloud providers utilized by the enterprise and the interface mechanisms employed (APIs, portals, etc.). Maintain these records current.	Identify and catalog all cloud providers utilized by the enterprise and the interface mechanisms employed (APIs, portals, etc.). Maintain these records current.
	Identify the functions, ports, protocols, and other services required for the company to interact with other companies' enterprise networks, maintain these records current.	Discuss and document the access mechanisms required for the company to interact with other companies' enterprise networks, maintain these records current.	Discuss and document the access mechanisms required for the company to interact with other companies' enterprise networks, maintain these records current.

PSO Cybersecurity Standards – Identify (2 / 4)

	High Tier	Middle Tier	Low Tier
ID.AM-5: Resources are prioritized based on their classification, criticality, and business value	Identify and prioritize production components and functions based on their criticality and business value.	Identify and prioritize production components and functions based on their criticality and business value.	
ID.AM-6: Cybersecurity roles and responsibilities are established	Establish and maintain personnel cybersecurity roles and responsibilities.	Establish and maintain personnel cybersecurity roles and responsibilities.	Establish a central point of contact for coordination of cybersecurity concerns and initiatives within the business.
	Establish a designated cybersecurity response coordinator.	Establish a designated cybersecurity response coordinator.	Establish a designated cybersecurity response coordinator.
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Identify and prioritize supporting services for critical businesses processes and components.		
	Identify alternate and redundant supporting services for critical production system processes and components.	Identify alternate and redundant supporting services for critical production system processes and components.	Understand single points of failure within the production environment and identify plan to recover systems if compromised.
	Implement Comprehensive Business Continuity Planning addressing all aspects of IT infrastructure and cybersecurity.	Implement Business Continuity Planning addressing critical services delivered by IT infrastructure	
ID.BE-5: Resilience requirements to support delivery of critical services are established	Define Recovery Time Objective and Recovery Point Objective for the resumption of essential business operations after a man made or natural disaster.	Define Recovery Time Objective and Recovery Point Objective for the resumption of essential business operations after a man made or natural disaster.	Understand which applications, services, and data are critical to core business functions, and estimated timeline to restore them in the event of a disaster.

PSO Cybersecurity Standards – Identify (3 / 4)

	High Tier	Middle Tier	Low Tier
ID.GV-1: Organizational cybersecurity policy is established and communicated	Develop and disseminate a security policy that provides an overview of the security requirements for the enterprise, including: roles and responsibilities, organizational entities accountable for different aspects of security (technical, physical, cyber, etc.), management commitment, etc. Ensure the security policy is approved by a senior official with responsibility and accountability for the risk being incurred by the enterprise.	Develop and disseminate a security policy that provides an overview of the security requirements for the enterprise, including: roles and responsibilities, organizational entities accountable for different aspects of security (technical, physical, cyber, etc.), management commitment, etc. Ensure the security policy is approved by a senior official with responsibility and accountability for the risk being incurred by the enterprise.	
	Establish and maintain a data management policy. Address data sensitivity, handling of data, data retention limits, and disposal requirements based on sensitivity and retention standards for the enterprise. (In particular, address PII governance to mitigate risk on the network.)	Establish and maintain a data management policy. Address data sensitivity, handling of data, data retention limits, and disposal requirements based on sensitivity and retention standards for the enterprise. (In particular, address PII governance to mitigate risk on the network.)	Understand the risk that PII and other sensitive data presents for the business, discuss with company employees. Implement measures to delete this data from the environment when no longer required..
ID.GV-3: Legal and regulatory requirements regarding cybersecurity are understood and managed	Ensure that legal and regulatory requirements affecting cybersecurity and data privacy are understood and managed.	Ensure that legal and regulatory requirements affecting cybersecurity and data privacy are understood and managed.	Ensure that legal and regulatory requirements affecting cybersecurity and data privacy are understood and managed.
ID.RA-1: Asset vulnerabilities are identified and documented	Perform routine (annual) vulnerability scanning and penetration testing (internal and external) to identify and remediate asset vulnerabilities within the enterprise. Perform external vulnerability scanning every 6 months.	Perform biennial periodic vulnerability scanning and penetration testing (internal and external), to identify asset vulnerabilities within the enterprise. Perform external vulnerability scanning every 6 months.	Perform an annual external vulnerability scan to identify asset vulnerabilities within the enterprise.

PSO Cybersecurity Standards – Identify (4 / 4)

	High Tier	Middle Tier	Low Tier
ID.RA-4: Potential business impacts and likelihoods are identified	Perform annual business continuity planning that addresses cybersecurity threats and associated business responses to maintain operations.	On an annual basis, conduct and document criticality reviews of the enterprise that define the likelihood and potential adverse impacts to operations, assets, and individuals if compromised or disabled.	Conduct annual "Tabletop" business response to natuaral or manmade disasters to recover and maintain business operations.
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Represent cyber related concerns within larger corporate risk management processes. If no process in place, stand up a risk management process that addresses IT Infrastructure and cybersecurity risks	Represent cyber related concerns within larger corporate risk management processes. If no process in place, stand up a risk management process that addresses IT Infrastructure and cybersecurity risks	Identify IT infrastructure and cybersecurity risks, risk mitigators, and communicate this information to key stakeholders.
ID.SC-2: Suppliers and third party partners are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Employ a Vendor Risk Management Solution that monitors vendors for external network vulnerabilities, incorporates periodic vendor survey (to assess internal network cyber standards), and track deficiency remediation	Employ a Vendor Risk Management Solution that monitors vendors for external network vulnerabilities; inform vendors of vulnerabilities and track deficiency remediation	Discuss cybersecurity with vendor partners to understand the extent to which they prioritize cybersecurity.
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	Require that critical IT vendors (MSPs and other IT services companies) provide 3rd party audits, inspection reports, or self-attestation for meeting the PSO Standards at the High Level to provide assurances of the practices they employ to prevent cyber attack of their own networks, and prevent disruptions to downstream clients.	Require that critical IT vendors (MSPs and other IT services companies) provide 3rd party audits, inspection reports, or self-attestation for meeting the PSO Standards at the High Level to provide assurances of the practices they employ to prevent cyber attack of their own networks, and prevent disruptions to downstream clients.	Require that critical IT vendors (MSPs and other IT services companies) provide 3rd party audits, inspection reports, or self-attestation for meeting the PSO Standards at the High Level to provide assurances of the practices they employ to prevent cyber attack of their own networks, and prevent disruptions to downstream clients.
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	Identify and document key personnel from suppliers and third-party partners (for both products and services) to include as stakeholders in response and recovery planning activities.	Identify and document key personnel from suppliers and third-party partners (for both products and services) to include as stakeholders in response and recovery planning activities.	Identify and document key personnel from suppliers and third-party partners (for both products and services) to include as stakeholders in response and recovery planning activities.

PSO Cybersecurity Standards – Protect (1 / 7)

	High Tier	Middle Tier	Low Tier
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Establish and manage identification mechanisms and credentials for users and devices. Implement automated mechanisms where feasible to support the management and auditing of information system credentials.	Establish and manage identification mechanisms and credentials for users and devices. Implement automated mechanisms where feasible to support the management and auditing of information system credentials.	Establish and manage identification mechanisms and credentials for users of all business IT systems.
	Monitor the enterprise for atypical use of system credentials. Credentials associated with significant risk are disabled. (Example solutions: Microsoft ATA, IBM Qradar, CyberArc, etc.)	Monitor the enterprise for atypical use of system credentials. Credentials associated with significant risk are disabled. (Example solutions: Microsoft ATA, IBM Qradar, CyberArc, etc.)	
	Deactivate system credentials after a specified time period of inactivity (2 months suggested), unless this would result in a compromise to safe operation of the process.	Deactivate system credentials after a specified time period of inactivity (2 months suggested), unless this would result in a compromise to safe operation of the process.	
PR.AC-2: Physical access to assets is managed and protected	Maintain and review visitor access records to enterprise facilities.	Maintain and review visitor access records to enterprise facilities.	
	Spaces and enclosures containing IT infrastructure equipment are locked.	Spaces and enclosures containing IT infrastructure equipment are locked, where possible. Server rooms must be locked.	Spaces and enclosures containing IT infrastructure equipment are locked, where possible.
	For facilities with computer-enabled physical access controls, mechanical access mechanisms exist to access critical spaces during emergencies (mechanical keys).	For facilities with computer-enabled physical access controls, mechanical access mechanisms exist to access critical spaces during emergencies (mechanical keys).	For facilities with computer-enabled physical access controls, mechanical access mechanisms exist to access critical spaces during emergencies (mechanical keys).
PR.AC-3: Remote access is managed	Allow remote access only through secure (incorporating MFA), approved, and managed access mechanisms. (Example: VPN with MFA)	Allow remote access only through secure (incorporating MFA), approved, and managed access mechanisms. (Example: VPN with MFA)	Allow remote access only through secure (incorporating MFA), approved, and managed access mechanisms. (Example: VPN with MFA)

PSO Cybersecurity Standards – Protect (2 / 7)

	High Tier	Middle Tier	Low Tier
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Implement automated mechanisms where feasible to support the management of system user accounts, including the disabling, auditing, notification, and removal of user accounts.	Implement automated mechanisms where feasible to support the management of system user accounts, including the disabling, auditing, notification, and removal of user accounts.	
	Only assign users the minimum rights they require to do their job.	Only assign users the minimum rights they require to do their job.	Only assign users the minimum rights they require to do their job.
	Limit, document, and explicitly authorize privileged user access to enterprise systems (Domain Admin, Server, Workstation). Audit the execution of privileged functions.	Limit, document, and explicitly authorize privileged user access to enterprise systems (Domain Admin, Server, Workstation). Audit the execution of privileged functions.	Limit, document, and explicitly authorize privileged user access to business systems (Domain Admin, Server, Workstation). Audit the execution of privileged functions.
	Monitor system usage for atypical use. Disable and investigate accounts of users posing a significant risk.	Add to standard above in AC1	
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Network segmentation is implemented within the enterprise.	Network segmentation is implemented within the enterprise where possible.	Network segmentation is implemented within the business network for Guest / OT. Add guidance that addresses potential VLANs for low (guest, SCADA, etc.)
	Operational Technology / SCADA networks are isolated from production (routable) networks, to the maximum extent possible.	Operational Technology / SCADA networks are isolated from production (routable) networks, to the maximum extent possible.	Operational Technology / SCADA networks are isolated from production (routable) networks, to the maximum extent possible.
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	Perform background checks for new employees, prior to authorizing access to IT systems. Segment (IT, Finance, core groups, office workers?)	Perform background checks for new employees, prior to authorizing access to IT systems.	Perform background checks for new employees, prior to authorizing access to IT systems.
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Implement Multi-Factor Authentication on all enterprise systems, to include admin access to workstations, remote network access, servers, infrastructure, critical applications, user accounts, cloud systems.	Implement Multi-Factor Authentication on all enterprise systems, to include admin access to workstations, remote network access, servers, infrastructure, critical applications, user accounts, cloud systems.	Implement Multi-Factor Authentication on all enterprise systems, to include admin access to workstations, remote network access, servers, infrastructure, critical applications, user accounts, cloud systems.

PSO Cybersecurity Standards – Protect (3 / 7)

	High Tier	Middle Tier	Low Tier
PR.AT-1: All users are informed and trained	Implement a security awareness program that provides quarterly training on cybersecurity topics.	Implement a security awareness program that provides quarterly training on cybersecurity topics. Incorporate phishing and social engineering awareness in this training.	Implement a security awareness program that provides quarterly training on cybersecurity topics. Incorporate phishing and social engineering awareness in this training.
	Implement phishing and social engineering awareness in this training, along with monthly simulated phishing testing for all users. Remediate failures with corrective training.		
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	Ensure that providers of external system services comply with defined security requirements. Monitor and audit external service providers for security compliance.	Ensure that providers of external system services comply with defined security requirements. Monitor and audit external service providers for security compliance.	
PR.AT-4: Senior executives understand their roles and responsibilities	Senior executives receive regular, recurring training on whaling awareness and prevention to include simulated whaling / social engineering tests.	Senior executives receive regular, recurring training on whaling awareness and prevention.	Senior executives receive training on whaling awareness and prevention.
	Senior executives are briefed on legal / regulatory requirements regarding cybersecurity.	Senior executives are briefed on legal / regulatory requirements regarding cybersecurity.	Senior executives are briefed on legal / regulatory requirements regarding cybersecurity.
PR.DS-1: Data-at-rest is protected	Implement procedures and technologies to ensure all data at rest is encrypted on all workstations and servers (on premise and in the cloud).	Implement procedures and technologies to ensure all data at rest is encrypted on all workstations and servers (on premise and in the cloud).	Implement procedures and technologies to ensure all data at rest is encrypted on all workstations and servers (on premise and in the cloud).
PR.DS-2: Data-in-transit is protected	Implement procedures and technologies to ensure that sensitive data in transit is protected via encryption.	Implement procedures and technologies to ensure that sensitive data in transit is protected via encryption.	Ensure that sensitive data in transit is protected via encryption where existing services and applications allow it (on premisis and in the cloud).

PSO Cybersecurity Standards – Protect (4 / 7)

	High Tier	Middle Tier	Low Tier
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Decommissioned assets are either forensically wiped prior to transfer/sale.	Decommissioned assets are either forensically wiped prior to transfer/sale.	Decommissioned assets are either forensically wiped prior to transfer/sale.
	Ensure that disposal actions are approved, tracked, documented, and verified.	Ensure that disposal actions are approved, tracked, documented, and verified.	
PR.DS-4: Adequate capacity to ensure availability is maintained	Ensure that resources are maintained for enterprise systems to ensure adequate memory, processing, network speeds, etc.	Ensure that resources are maintained for enterprise systems to ensure adequate memory, processing, network speeds, etc.	Ensure that resources are maintained for business systems to ensure adequate memory, processing, network speeds, etc.
	Protect enterprise systems against, or limit the effects of, denial of service attacks.	Protect enterprise systems against, or limit the effects of, denial of service attacks.	
PR.DS-5: Protections against data leaks are implemented	Implement Data Loss Protection solutions within the enterprise (for cloud solutions and on premisis systems) to detect and terminate accidental and/or deliberate data exfiltration.	Implement Data Loss Protection solutions for cloud offering to detect and terminate accidental and/or deliberate data exfiltration.	
PR.DS-7: The development and testing environment(s) are separate from the production environment	Implement off-line development and testing systems for implementing and testing changes to enterprise systems.	Implement off-line development and testing systems for implementing and testing changes to enterprise systems.	
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	Enterprise systems are patched and kept up to date. All unused services are disabled	Enterprise systems are patched and kept up to date. All unused services are disabled	Enterprise systems are patched and kept up to date. All unused services are disabled
	An automated endpoint detection and response service is deployed to all endpoints and kept up to date.	Antivirus or automated endpoint detection and response service protection is deployed to all endpoints and kept up to date.	Antivirus or automated endpoint detection and response service protection is deployed to all endpoints and kept up to date.
	Local operating system firewall implemented to allow only needed services in.	Local operating system firewall implemented to allow only needed services in.	Local operating system firewall implemented to allow only needed services in.

PSO Cybersecurity Standards – Protect (5 / 7)

	High Tier	Middle Tier	Low Tier
PR.IP-2: A System Development Life Cycle to manage systems is implemented	Include security requirements in the acquisition process of enterprise systems and their components.	Include security requirements in the acquisition process of enterprise systems and their components.	
	Ensure all SDLC components are up to date and covered by manufacturers support		
PR.IP-3: Configuration change control processes are in place	Implement configuration change control for enterprise systems and their components. Conduct security impact analyses in connection with change control reviews.	Implement configuration change control for enterprise systems and their components. Conduct security impact analyses in connection with change control reviews.	Implement configuration change control for businesss systems and their components. Conduct security impact analyses in connection with change control reviews.
	Test, validate, and document all changes to enterprise systems before implementing the changes on the operational system.	Test, validate, and document all changes to enterprise systems before implementing the changes on the operational system.	Where possible, test, validate, and document changes to enterprise systems before implementing the changes on the operational system.
PR.IP-4: Backups of information are conducted, maintained, and tested	Implement data backups of business critical applications and databases. Where possible, store these backups at a physically different site than their primary location and/or in the cloud NOTE: Local copy should also be maintained to ensure speedy recovery	Implement data backups of business critical applications and databases. Where possible, store these backups at a physically different site than their primary location and/or in the cloud.	Implement data backups of business critical applications and databases. Where possible, store these backups at a physically different site than their primary location and/or in the cloud.
	Verify the reliability and integrity of backups on a monthly basis.	Verify the reliability and integrity of backups on a monthly basis.	Verify the reliability and integrity of backups every 6 months.
	Ensure backups are 'air-gapped', such that compromise of Domain Administrator credentials will not allow criminals to destroy backups.	Ensure backups are 'air-gapped', such that compromise of Domain Administrator credentials will not allow criminals to destroy backups.	Ensure backups are 'air-gapped', such that compromise of Domain Administrator credentials will not allow criminals to destroy backups.

PSO Cybersecurity Standards – Protect (6 / 7)

	High Tier	Middle Tier	Low Tier
PR.IP-6: Data is destroyed according to policy	Ensure that enterprise system data is destroyed according to policy. Employ secure electronic sanitization techniques and e-wasting procedures for physical data repositories.	Ensure that enterprise system data is destroyed according to policy. Employ secure electronic sanitization techniques and e-wasting procedures for physical data repositories.	Employ secure electronic sanitization techniques and e-wasting procedures for physical data repositories.
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Develop and maintain full Incident Response and Disaster Recovery plans which integrate with the Business Continuity Plans. Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information.	Develop and maintain full Incident Response and Disaster Recovery plans which integrate with the Business Continuity Plans. Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information.	Develop and maintain full Incident Response and Disaster Recopvery plans, with 'table top' engagement on Business Continuity Planning. Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information.
PR.IP-10: Response and recovery plans are tested	Test disaster recovery plans annually to determine the effectiveness of the plans, and the readiness to execute the plans.	Test response and recovery plans biennially to determine the effectiveness of the plans, and the readiness to execute the plans.	"Tabletop" response and recovery plans biennially to determine the effectiveness of the plans, and the readiness to execute the plans.
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Human Resources personnel offboarding procedures incorporate notification of IT to ensure deactivation of the employee's user account and revoke access to physical sites, enterprise applications, and networks on the last day of employment.	Human Resources personnel offboarding procedures incorporate notification of IT to ensure deactivation of the employee's user account and revoke access to physical sites, enterprise applications, and networks on the last day of employment.	Human Resources personnel offboarding procedures incorporate notification of IT to ensure deactivation of the employee's user account and revoke access to physical sites, enterprise applications, and networks on the last day of employment.
	Audit records and spot check actual offboarding events to ensure compliance on a quarterly basis.	Audit records and spot check actual offboarding events to ensure compliance on a quarterly basis.	Audit records and spot check actual offboarding events to ensure compliance on a quarterly basis.

PSO Cybersecurity Standards – Protect (7 / 7)

	High Tier	Middle Tier	Low Tier
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Have servers log all remote access and configure disconnected sessions to auto logoff.	Have servers log all remote access and configure disconnected sessions to auto logoff.	Have servers log all remote access and configure disconnected sessions to auto logoff.
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Implement a Security Information and Event Monitoring (SIEM) to process event records from across the enterprise and alert on potentially problematic or malicious activity.	Implement a Security Information and Event Monitoring (SIEM) to process event records from across the enterprise and alert on potentially problematic or malicious activity.	
PR.PT-2: Removable media is protected and its use restricted according to policy	Implement controls to ensure the secure use of portable storage devices	Implement controls to ensure the secure use of portable storage devices	Implement controls to ensure the secure use of portable storage devices
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Implement atheniciation systems that enable enforcement of principle of least priviledge for infrastructure components (switches, firewalls, servers, workstations, etc.)	Implement authentication systems that enable enforcement of principle of least privilege for infrastructure components (switches, firewalls, servers, workstations, etc.)	Restrict access to infrastructure components to authorized administrators.
PR.PT-4: Communications and control networks are protected	A set of solutions are implemented to provide safe web browsing to users, protecting against malware, botnets, phishing, and targeted online attacks.	A set of solutions are implemented to provide safe web browsing to users, protecting against malware, botnets, phishing, and targeted online attacks.	A set of solutions are implemented to provide safe web browsing to users, protecting against malware, botnets, phishing, and targeted online attacks.

PSO Cybersecurity Standards – Detect (1 / 4)

	High Tier	Middle Tier	Low Tier
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Develop a baseline of network operations, traffic, and expected data flows for the enterprise. Document and maintain current in order to assist in detecting abnormal events.	Develop a baseline of network operations, traffic, and expected data flows for the enterprise. Document and maintain current in order to assist in detecting abnormal events.	
DE.AE-2: Detected events are analyzed to understand attack targets and methods	Implement automated mechanisms where feasible to review and analyze detected events within the enterprise (Microsoft ATA, Cisco AMP, Arctic Wolf, etc.).	Implement automated mechanisms where feasible to review and analyze detected events within the enterprise (Microsoft ATA, Cisco AMP, Arctic Wolf, etc.).	Review and analyze detected events within the organization's log aggregation tooling.
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	Integrate analysis of events where feasible with the analysis of vulnerability scanning information; performance data; production system monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity.	Integrate analysis of events where feasible with the analysis of vulnerability scanning information; performance data; production system monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity.	
	Implement a security information and event management system to automate the aggregation, analysis, and alerting of logs and event data.	Implement a security information and event management system to automate the aggregation, analysis, and alerting of logs and event data.	
DE.AE-4: Impact of events is determined	The actual or potential impacts of confirmed security events are fully investigated and understood, in order to inform post event risk mitigation activities.	The actual or potential impacts of confirmed security events are fully investigated and understood, in order to inform post event risk mitigation activities.	The actual or potential impacts of confirmed security events are fully investigated and understood, in order to inform post event risk mitigation activities.
DE.AE-5: Incident alert thresholds are established	Implement automated mechanisms where feasible to assist in the identification of security alert thresholds (account escalation, failed logon attempts, unauthorized access attempts, etc.)	Implement automated mechanisms where feasible to assist in the identification of security alert thresholds (account escalation, failed logon attempts, unauthorized access attempts, etc.)	Define alert thresholds for the business, review and maintain current on a quarterly basis.

PSO Cybersecurity Standards – Detect (2 / 4)

	High Tier	Middle Tier	Low Tier
DE.CM-1: The network is monitored to detect potential cybersecurity events	Utilize automated mechanisms to monitor for and report atypical usage of enterprise networks.	Utilize automated mechanisms to monitor for and report atypical usage of enterprise networks.	
	Conduct ongoing security status monitoring of enterprise networks to detect defined cybersecurity events and indicators of potential cybersecurity events	Conduct ongoing security status monitoring of enterprise networks to detect defined cybersecurity events and indicators of potential cybersecurity events	Conduct ongoing security status monitoring of business networks to detect defined cybersecurity events and indicators of potential cybersecurity events
	Monitor network communications at the external boundary of the system and at key internal boundaries within the system.	Monitor network communications at the external boundary of the system and at key internal boundaries within the system.	
	Implement automated mechanisms to support detection of cybersecurity events and generate actionable alerts based upon these events.	Implement automated mechanisms to support detection of cybersecurity events and generate actionable alerts based upon these events.	
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Conduct ongoing security status monitoring of enterprise facilities to detect physical security incidents.	Conduct ongoing security status monitoring of enterprise facilities to detect physical security incidents.	Conduct ongoing security status monitoring of the business facilities to detect physical security incidents.
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Ensure users do not have administrator rights to their workstations.	Ensure users do not have administrator rights to their workstations.	Ensure users do not have administrator rights to their workstations.
DE.CM-4: Malicious code is detected	Ensure all systems are protected by a centralized next generation antivirus solution that can alert IT of events.	Ensure all systems are protected by a centralized next generation antivirus solution that can alert IT of events.	
	Complete monthly (minimum) antivirus scans of all enterprise assets.	Complete monthly (minimum) antivirus scans of all enterprise assets.	Complete monthly (minimum) antivirus scans of all business assets.

PSO Cybersecurity Standards – Detect (3 / 4)

	High Tier	Middle Tier	Low Tier
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Conduct ongoing security status monitoring of external service providers and vendors that access enterprise systems.	Conduct ongoing security status monitoring of external service providers and vendors that access enterprise systems.	Conduct ongoing security status monitoring of external service providers and vendors that access enterprise systems.
	Monitor compliance of external providers and vendors with security policies and procedures, and contract security requirements	Monitor compliance of external providers and vendors with security policies and procedures, and contract security requirements	
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Monitor for unauthorized configuration changes to enterprise systems.	Monitor for unauthorized configuration changes to enterprise systems.	
	Monitor the enterprise for inventory discrepancies.	Monitor the enterprise for inventory discrepancies.	Monitor the enterprise for inventory discrepancies.
	Conduct ongoing security status monitoring on the enterprise networks for unauthorized personnel, connections, devices, access points, and software.	Conduct ongoing security status monitoring on the enterprise networks for unauthorized personnel, connections, devices, access points, and software.	Conduct ongoing security status monitoring on the enterprise networks for unauthorized personnel, connections, devices, access points, and software.
DE.CM-8: Vulnerability scans are performed	Conduct quarterly internal and monthly external vulnerability scans on enterprise systems where safe and feasible. Include analysis, remediation, and information sharing in the vulnerability scanning process.	Conduct quarterly internal and monthly external vulnerability scans on enterprise systems where safe and feasible. Include analysis, remediation, and information sharing in the vulnerability scanning process.	Conduct yearly internal and monthly external vulnerability scans on enterprise systems where safe and feasible. Include analysis, remediation, and information sharing in the vulnerability scanning process.
DE.DP-2: Detection activities comply with all applicable requirements	Ensure that detection activities (vulnerability scanning, monitoring, etc.) adhere to requirements for regulations or certifications required of the business (i.e. SOC2).	Ensure that detection activities (vulnerability scanning, monitoring, etc.) adhere to requirements for regulations or certifications required of the business (i.e. SOC2).	Ensure that detection activities (vulnerability scanning, monitoring, etc.) adhere to requirements for regulations or certifications required of the business (i.e. SOC2).
DE.DP-3: Detection processes are tested	Validate that event detection processes are operating as intended.	Validate that event detection processes are operating as intended.	Validate that event detection processes are operating as intended.

PSO Cybersecurity Standards – Detect (4 / 4)

	High Tier	Middle Tier	Low Tier
DE.DP-4: Event detection information is communicated	Communicate event detection information to defined personnel as part of the organization's incident response procedures.	Communicate event detection information to defined personnel as part of the organization's incident response procedures.	Communicate event detection information to defined personnel as part of the business' incident response procedures.
	Implement automated mechanisms and system generated alerts to support event detection communication.	Implement automated mechanisms and system generated alerts to support event detection communication.	
DE.DP-5: Detection processes are continuously improved	Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into detection process revisions (incident response plan).	Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into detection process revisions (incident response plan).	Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into detection process revisions (incident response plan).
	Leverage opportunites for assessment of monitoring and alerting tools deployed thorughout the enterprise (penetration testing) to evaluate and improve detection processes.	Leverage opportunites for assessment of monitoring and alerting tools deployed thorughout the enterprise (penetration testing) to evaluate and improve detection processes.	

PSO Cybersecurity Standards – Respond (1 / 3)

	High Tier	Middle Tier	Low Tier
RS.RP-1: Response plan is executed during or after an incident	Leverage company incident response plan during and/or after a cybersecurity event to guide response efforts and prioritization.	Leverage company incident response plan during and/or after a cybersecurity event to guide response efforts and prioritization.	Leverage company incident response plan during and/or after a cybersecurity event to guide response efforts and prioritization.
RS.CO-1: Personnel know their roles and order of operations when a response is needed	Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event response. Incorporate refresher training on responsibilities into annual training.	Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event response. Incorporate refresher training on responsibilities into annual training.	Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event response.
RS.CO-2: Incidents are reported consistent with established criteria	Ensure that incident reporting criteria, frequency, content, and person in charge of reporting are defined in advance for appropriate stakeholders. Execute this plan during a cybersecurity event.	Ensure that incident reporting criteria, frequency, content, and person in charge of reporting are defined in advance for appropriate stakeholders. Execute this plan during a cybersecurity event.	Ensure that incident reporting criteria, frequency, content, and person in charge of reporting are defined in advance for appropriate stakeholders. Execute this plan during a cybersecurity event.
	Ensure that there is clarity on how an organization will report incidents to: government agencies, the board, customers, employees, vendors. Action upon reporting requirements.	Ensure that there is clarity on how an organization will report incidents to: government agencies, the board, customers, employees, vendors. Action upon reporting requirements.	Ensure that there is clarity on how an organization will report incidents to: government agencies, the board, customers, employees, vendors. Action upon reporting requirements.
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Share anonymized cybersecurity event information voluntarily, as appropriate and anonymously if requested by the organization, with the PSO to achieve broader cybersecurity situational awareness.	Share anonymized cybersecurity event information voluntarily, as appropriate and anonymously if requested by the organization, with the PSO to achieve broader cybersecurity situational awareness.	Share anonymized cybersecurity event information voluntarily, as appropriate and anonymously if requested by the organization, with the PSO to achieve broader cybersecurity situational awareness.

PSO Cybersecurity Standards – Respond (2 / 3)

	High Tier	Middle Tier	Low Tier
RS.AN-1: Notifications from detection systems are investigated	Investigate cybersecurity-related notifications generated from detection systems deployed in the environment (consistent with organization's specified thresholds for investigation as defined by risk management processes).	Investigate cybersecurity-related notifications generated from detection systems deployed in the environment (consistent with organization's specified thresholds for investigation as defined by risk management processes).	Investigate cybersecurity-related notifications generated from detection systems deployed in the environment (consistent with organization's specified thresholds for investigation as defined by risk management processes).
	Implement automated mechanisms to assist in the identification, analysis, and triage of cybersecurity-related notificaitons (SIEM, SOC, etc).	Implement automated mechanisms to assist in the identification, analysis, and triage of cybersecurity-related notificaitons (SIEM, SOC, etc).	
RS.AN-2: The impact of the incident is understood	Evaluate the real-time, wholistic impact of the event for the business (2nd and 3rd order effects of IT system disruptions), communicate to key stakeholders within the company.	Evaluate the wholistic impact of the event for the business (2nd and 3rd order effects of IT system disruptions), communicate to key stakeholders within the company.	Evaluate the wholistic impact of the event for the business (2nd and 3rd order effects of IT system disruptions), communicate to key stakeholders within the company.
RS.AN-3: Forensics are performed	Conduct forensic analysis on collected event information to determine root cause of the incident and appropriate corrective actions to prevent recurrence.	Conduct forensic analysis on collected event information to determine root cause of the incident and appropriate corrective actions to prevent recurrence.	Conduct forensic analysis on collected event information to determine root cause of the incident and appropriate corrective actions to prevent recurrence.
RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	Implement and execute a formalized vulnerability risk management process to incorporate processing, analyzing, prioritizing, and remediating vulnerabilities identified from internal and external sources.	Implement and execute a formalized vulnerability risk management process to incorporate processing, analyzing, prioritizing, and remediating vulnerabilities identified from internal and external sources.	Implement and execute a formalized vulnerability risk management process to incorporate processing, analyzing, prioritizing, and remediating vulnerabilities identified from internal and external sources.

PSO Cybersecurity Standards – Respond (3 / 3)

	High Tier	Middle Tier	Low Tier
RS.MI-1: Incidents are contained	Incorporate procedures, measures, and activities into the organization's response plans to contain the cybersecurity event and minimize overall impact on the environment. (Kerberos rolls, password resets, etc.)	Incorporate procedures, measures, and activities into the organization's response plans to contain the cybersecurity event and minimize overall impact on the environment. (Kerberos rolls, password resets, etc.)	Incorporate procedures, measures, and activities into the organization's response plans to contain the cybersecurity event and minimize overall impact on the environment. (Kerberos rolls, password resets, etc.)
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Ensure that vulnerabilities identified while responding to a cybersecurity incident are mitigated or documented as accepted risks.	Ensure that vulnerabilities identified while responding to a cybersecurity incident are mitigated or documented as accepted risks.	Ensure that vulnerabilities identified while responding to a cybersecurity incident are mitigated or documented as accepted risks.
RS.IM-1: Response plans incorporate lessons learned	Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.	Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.	Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.
RS.IM-2: Response strategies are updated	Update the response plans to address changes to the organization, production system, enterprise architecture, enterprise applications, attack vectors, environment of operation, and/or industry lessons learned and problems encountered during plan implementation, execution, or testing.	Update the response plans to address changes to the organization, production system, enterprise architecture, enterprise applications, attack vectors, environment of operation, and/or industry lessons learned and problems encountered during plan implementation, execution, or testing.	Update the response plans to address changes to the organization, production system, enterprise architecture, enterprise applications, attack vectors, environment of operation, and/or industry lessons learned and problems encountered during plan implementation, execution, or testing.

PSO Cybersecurity Standards – Recover (1 / 1)

	High Tier	Middle Tier	Low Tier
RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	Execute the recovery plan during or after a cybersecurity incident to minimize loss of operational continuity.	Execute the recovery plan during or after a cybersecurity incident to minimize loss of operational continuity.	Execute the recovery plan during or after a cybersecurity incident to minimize loss of operational continuity.
RC.IM-1: Recovery plans incorporate lessons learned	Update the recovery plan to address lessons learned, changes to the environment, and problems encountered during plan execution or testing.	Update the recovery plan to address lessons learned, changes to the environment, and problems encountered during plan execution or testing.	Update the recovery plan to address lessons learned, changes to the environment, and problems encountered during plan execution or testing.
RC.CO-1: Public relations are managed	Centralize media and public relations to one individual or group with authority to speak for the organization and vet information for release to employees, law enforcement, customers, vendors, and the general public. Ensure this person(s) remain up to date on status of the incident and recovery.	Centralize media and public relations to one individual or group with authority to speak for the organization and vet information for release to employees, law enforcement, customers, vendors, and the general public. Ensure this person(s) remain up to date on status of the incident and recovery.	Centralize media and public relations to one individual or group with authority to speak for the organization and vet information for release to employees, law enforcement, customers, vendors, and the general public. Ensure this person(s) remain up to date on status of the incident and recovery.
RC.CO-2: Reputation is repaired after an incident	Provide leadership with a technical assessment of the incident attack vectors, countermeasures deployed to prevent future incidents, and assurances that the criminals are out of the network to assist the business in repairing reputational harm.	Provide leadership with a technical assessment of the incident attack vectors, countermeasures deployed to prevent future incidents, and assurances that the criminals are out of the network to assist the business in repairing reputational harm.	Provide leadership with a technical assessment of the incident attack vectors, countermeasures deployed to prevent future incidents, and assurances that the criminals are out of the network to assist the business in repairing reputational harm.
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	Ensure that all organizational stakeholders remain fully updated on current and projected limitations, outages, or operational consequences of the event along with projected timeline for full restoration of services.	Ensure that all organizational stakeholders remain fully updated on current and projected limitations, outages, or operational consequences of the event along with projected timeline for full restoration of services.	Ensure that all organizational stakeholders remain fully updated on current and projected limitations, outages, or operational consequences of the event along with projected timeline for full restoration of services.