ARLINGTON

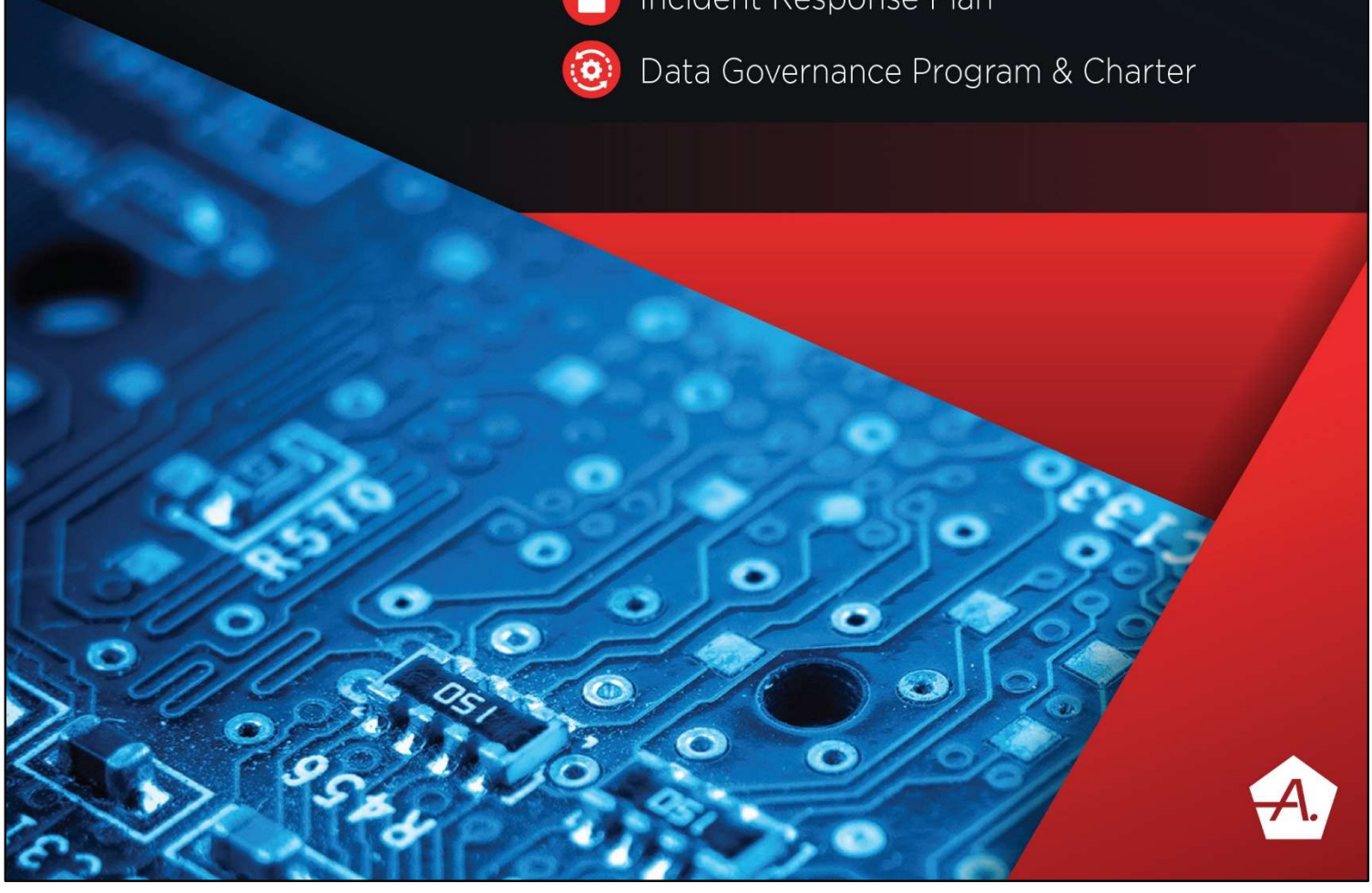
DEDICATED TO DEFENSE

HAVE QUESTIONS?

Talk to an ASP Expert at 703-591-3466

Listed below are selected excerpts from the following policies, procedures, programs, and plans from the Arlington Security Portal (ASP):

- Portable Storage Devices Policy & Procedures
- Penetration Testing Policy & Procedures
- Incident Response Plan
- Data Governance Program & Charter



[Company Name] Portable Storage Devices Policy and Procedures

Official Policy Title:	
Responsible Party:	
Approval Party:	
Effective Date:	
Last Update:	
Version Number:	
Policy Framework:	**Developed in accordance with NIST Special Publication (SP) 800 Series - https://csrc.nist.gov/publications/sp800**
Mapping	**(1). NIST SP 800-53, rev. 5 [NIST AC-20(2,5)], [NIST MP-6(3)], [NIST MP-7(b)]**

Introduction

The Portable Storage Devices policy and procedures referenced within this document defines the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, this policy and procedures document is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Portable Storage Devices policy and procedures are to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Portable Storage Devices policy and procedures is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity.*

- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

Per NIST SP 800-53, rev. 5, a Portable Storage Devices is defined as "A system component that can communicate with and be added to or removed from a system or network and that is limited to data storage—including text, video, audio or image data—as its primary function (e.g., optical discs, external or removable hard drives, external or removable solid-state disk drives, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks)".

Policy

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within this policy, or within a separate set of standard operating procedures (SOP), as needed.

Portable Storage Devices Risks

Though portable storage devices are seen as inexpensive, relatively easy-to-use and acquire, they also offer tremendous challenges in terms of protecting the safety and security of highly sensitive and confidential information for [company name]. Such challenges include the loss, theft, or misplacement of these devices because of their small size. Additionally, most of these devices do not come pre-configured with any type of encryption measures. Moreover, such devices have been known to transmit dangerous malware as they're often given away at conferences, trade shows, seminars, and other public gatherings. More specifically, notable security breaches have occurred in recent years at many organizations as employees have unknowingly inserted virus infected USB drives into their computers. It's important to note that numerous security threats in recent years have been tracked to malicious codes loaded onto USB external thumb drives, thus the importance of obtaining portable storage devices from trusted sources is critical.

Restricted Use of Portable Storage Devices [NIST AC-20(2)]

It is the strict policy of [company name] to *restrict* the use of the portable storage devices for only a valid and justified business reason, for which such devices may only be used temporarily, with a documented timeframe applied. Unless specifically authorized, at no time may any employee use such devices for extracting and receiving any type of [company name] information, and specifically not any type of highly sensitive and confidential information.

Prohibited Use of Portable Storage Devices [NIST AC-20(5)]

It is the strict policy of [company name] to *prohibit* the use of the portable storage devices, unless explicitly authorized for a valid and justified business reason, for which such devices may only be used temporarily, with a documented timeframe applied.

Prohibited Use of Portable Storage Devices with No Identifiable Owner [NIST MP-7(b)]

It is the strict policy of [company name] to *prohibit* the use of portable storage devices when such devices have no identifiable owner.

Acquiring Portable Storage Devices

If portable storage devices have been approved for use, they are to be acquired from trusted sources and are to have never been previously used. Any such devices that have shown to be tampered with are to be immediately returned to the vendors who supplied them. Portable storage devices procured outside of the company, such as items purchased by employees or obtained through any other channels (i.e., trade shows, conferences, seminars, etc.) are always prohibited from use.

Nondestructive Techniques [NIST MP-6(3)]

[Company name] is to apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to any organizational-owned information systems when the following circumstances warrant such sanitization techniques: [Define what circumstances require sanitization of portable storage devices prior to their use].

Management of Portable Storage Devices

The stated policy, while addressing the use and application of various types of portable storage devices, is to also address the management of other types of portable storage devices that are considered outside the scope of the aforementioned items. For example, desktops, laptops, servers, tape backups, and more, are all examples of assets that contain data and information – hence media – on them, that are exempt.

[Company Name] Penetration Testing Policy and Procedures

Official Policy Title:	
Responsible Party:	
Approval Party:	
Effective Date:	
Last Update:	
Version Number:	
Policy Framework:	**Developed in accordance with NIST Special Publication (SP) 800 Series - https://csrc.nist.gov/publications/sp800 (NIST SP 800-53, rev. 5)**
Mapping	**(1). NIST SP 800-53, rev. 5 [NIST CA-8], [NIST SA-11(5)]**

Introduction

The Penetration Testing policy and procedures referenced within this document define the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, this policy and procedures document is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Penetration Testing policy and procedures are to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Penetration Testing policy and procedures is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity.*

- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

Additionally, for policy scope purposes, "penetration testing" is defined as the following: A method of testing where testers target individual binary components or the application to determine whether intra or inter component vulnerabilities can be exploited to compromise the application, its data, or its environment resources.

Policy

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within this policy, or within a separate set of standard operating procedures (SOP), as needed.

Testing Methodology

Implement a methodology for penetration testing that includes the following:

- Is based on industry-accepted penetration testing approaches.
- Includes coverage for the entire in-scope environment and critical systems.
- Includes testing from both inside and outside the network.
- Includes testing to validate any segmentation and scope-reduction controls.
- Defines application-layer penetration tests to include, at a minimum, issues and risks found during vulnerability scanning.
- Defines network-layer penetration tests to include components that support network functions as well as operating systems.
- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months.
- Specifies retention of penetration testing results and remediation activities results.
- Is to be performed at least annually and after any significant infrastructure or application upgrades or modification.
- Is to be performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester is to exist.
- Exploitable vulnerabilities found during penetration testing are to be corrected and testing is repeated to verify the corrections.

Testing Protocol

[Company name] is to perform penetration testing with the following protocols:

- **Schedule** – Penetration testing is to be scheduled to align with the evolution of [company name]'s technology solutions, which may result in new exploitable weaknesses. Penetration is not to be generally completed against live production systems as the impact of the testing may in some cases be detrimental to the stability or performance of the system. Rather, penetration testing is to be generally completed against a full duplicate of a system or of the template / model system if possible.
    - Penetration testing is to be aligned with major application version releases, for which the following are to be considered activities that may trigger a penetration test:
        - Adoption of a new operating system, major release of operating system, database technology, or third-party application as part of the standard build for servers at [company name].
        - A new major release of software or third-party software integral to [company name]'s environment.
    - The following events may also trigger a penetration testing event:
    - Indication of a breach of a [company name] system for which the entry point is not well defined or understood.
    - Information that would lead [company name] to believe that a system is vulnerable to a given attack or family of attacks.
- **Approach** – Penetration testing is to be conducted by [company name] SMEs and / or third-party resources as necessary to develop confidence that [company name] maintains an appropriate information security posture.
- **Tool Sets and Execution** – [Company name] is to use industry standard penetration testing tools, and additional supporting tool sets as necessary.
- **Notification and Execution** - Relevant subject matter experts (i.e., system, software, etc.) are to be engaged in the process in advance and are aware that the testing is occurring. In the event that a test must be executed against a production system, it will be completed during a maintenance window with appropriate change request documentation.

Red Team Exercises [NIST CA-8(2)]

[Company name] is to employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement:

Red Team Exercise	General Description of Exercise	Responsible Party

Facility Penetration Testing [NIST CA-8(3)]

[Company name] is to employ a penetration testing process that includes [Assignment: organization-defined frequency] [Selection: announced; unannounced] attempts to bypass or circumvent controls associated with physical access points to the facility.

Developer Testing and Evaluation Penetration Testing [NIST SA-11(5)]

[Company name] is to require the developer of the system, system component, or system service to perform penetration testing: (a) At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; and (b) Under the following constraints: [Assignment: organization-defined constraints].

[Company Name] Incident Response Plan

Official Policy Title:	
Responsible Party:	
Approval Party:	
Effective Date:	
Last Update:	
Version Number:	
Policy Framework:	**Developed in accordance with NIST Special Publication (SP) 800 Series - https://csrc.nist.gov/publications/sp800**
Mapping	**NIST SP 800-53, rev. 5 [IR-1 to IR-9]**

Introduction

The Incident Response Plan referenced within this document defines the security measures implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems that are owned, operated, and/or maintained by the organization. Additionally, the Incident Response Plan is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Incident Response Plan is to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Incident Response Plan is to outline the organization's information security objectives, protect organizational assets, while also defining plans, rules, and practices to be implemented for helping ensure the Confidentiality, Integrity, and Availability (CIA) of information systems when a suspected, or actual incident, occurs. Please note for purposes of this document, "policy" and "procedures" are defined as the following:

- Policy: *Statements, rules or assertions that specify the correct or expected behavior of an entity.*

- Procedures: *How the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.*

Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

Additionally, per NIST, an 'Incident' is defined as the following: *"An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."*

Furthermore, per DFARS 7012, a 'cyber incident' means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Plan [NIST IR-8]

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within the Incident Response Plan, or within a separate set of standard operating procedures (SOP), as needed:

Team Structure

A documented Incident Response Team (IRT) is to have clear roles and responsibilities for properly responding to any incident that can impact the confidentiality, integrity, and availability (CIA) of [company name]'s information systems. Additionally, the IRT is to be built around the needs of the organization, one that is scalable, flexible, and includes the use of any outsourced entities for helping to aid and facilitate the entire incident response and reporting plan. As such, the IRT structure consists of the following titles and related roles and responsibilities:

<u>Senior Management:</u>

- The designated individual(s) will be the most important public face of the organization in relation to the security incident.
- Directly deliver critical public announcements.
- Having primary responsibility for mandatory breach reporting to regulators.
- Looked upon for leadership and direction in a time of crisis.

- Actively reaffirm the corporate values and culture of the organization as the security incident unfolds.

Incident Response Manager:

- Responsibility and authority for oversight of any suspected or actual incident that does arise.
- Assessing severity of incident and assembling appropriate team members to act.
- Gathering all necessary information from subject matter experts.
- Making essential decisions on all phases of incident response.
- Act as the lead voice, internally, regarding communications for all essential decisions on all phases of the incident lifecycle.
- Coordinating and directing all aspects of the incident response efforts, from initial incident alert to final resolution and post-incident reporting activities.

Incident Responders/Handlers/Coordinators:

- Collect intrusion artifacts (e.g., source code, malware, trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the organization.
- Coordinate and provide expert technical support to organizational-wide cyber defense technicians to resolve cyber defense incidents.
- Coordinate incident response functions.
- Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain a strong awareness of cyber defense threat conditions and determine which security issues may have an impact on the organization.
- Perform cyber defense trend analysis and reporting.
- Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on organizational systems.
- Receive and analyze network alerts from various sources within the organization and determine possible causes of such alerts.
- Write and publish after-action reviews.

Forensic Analysts:

- Conduct analysis of log files, evidence, and other information to determine the best methods for identifying the perpetrator(s) of a network intrusion.
- Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.
- Provide a technical summary of findings in accordance with established reporting procedures.
- Examine recovered data for information of relevance to the issue at hand.
- Perform file signature analysis.
- Perform file system forensic analysis.
- Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the organization.

Security Analysts:

- Monitor computer networks and systems for threats and security breaches.
- Install, alter, and update security software and firewalls.
- Test systems for potential vulnerabilities.
- Develop systems and processes for security best practices throughout the organization.
- Prepare reports on security incidents and changing responses.

Human Resources:

- Provide guidance as to how best to handle situations involving employees for a given incident.
- Advising on policies that were violated or that have to be adhered to, before taking any action on the employee.

Legal:

- Maintaining the confidentiality of the incident investigation.
- Protecting applicable internal communications under the attorney-client privilege and work product protections.
- Anticipating and preparing for litigation and other legal risks.
- Assist in identifying legal obligations following any data incident, including any notification requirements.
- Initiate and drive many of the actions needed to gather, secure, and analyze the data breach.
- Oversee overall legal work involved, and coordinate, manage and advise other external parties involved in the incident response team.

Public Relations: [NIST IR-4(15)]

- Oversee both internal and external incident response communication throughout the incident lifecycle.
- Determine which communication channels will be used for the respective audiences.
- Ensure that the incident response team, the organization, external stakeholders, customers, and the public are properly informed.

Local/State/Federal Agency Liaison:

- Maintain an up-to-date database on all relevant law enforcement agencies.
- As necessary, coordinate all communication efforts with law enforcement agencies.

Client Liaison:

- Work specifically with any clients that have been impacted by the incident.
- Maintain effective dialogue in terms of keeping clients abreast of various aspects of the incident.

Internal Incident Response Team (IRT) Personnel Matrix [NIST IR-4(11)]

IRT Title	Name(s)	Contact Information	Additional Comments
Senior Management			
Incident Response Manager			
Incident Responders/Handlers/Coordinators			
Forensic Analysts			
Security Analysts			
Human Resources			
Legal			
Public Relations			
Local/State/Federal Agency Liaison			
Client Liaison			

Third-Party Incident Response Team (IRT) Personnel Matrix

Name of Third Party Provider:	XYZ Managed Services		
Address	123 Main Street, Dallas, Texas 75205		
Services Provided	Managed network devices consisting of management of all firewalls, routers, switches, and load balancers. Because of their responsibilities to the network, the XYZ Managed Services is responsible for responding to incidents affecting [company name]'s network.		
Name of Personnel	**Title**	**Contact Information**	**Role and Responsibility of the Incident Response Team**
Jessie Delgado	Network Engineer	Jdelgado@xyzmanagedservices.com	Responding to any incidents against [company name]'s network and remediating as necessary for ensuring the continued uptime and overall safety of the network.

Security Operations Center [NIST IR-4(14)]

[Company name] is to establish and maintain a security operations center.

Incident Response Training [NIST IR-2]

A vitally important component of [company name]'s incident response measures is ensuring that all employees and other in-scope personnel are aware of response mechanisms and other protocols regarding such issues. As such, the [company name] security awareness training program is to include mandated provisions regarding the incident response practices. Additionally, any other incident response training deemed essential for employees and other in-scope personnel is to be conducted as necessary. Therefore, for training measures regarding incident response, it can also be conducted as a stand-alone initiative – separate from the organization's enterprise-wide training, if necessary.

Incident Response Training Matrix

Personnel Type	Training Provided	Format
Employees	Incident Response Training is provided as part of the company's annual security awareness training, and provided as necessary when additional circumstances merit such training	Online portal that employees can log into for annual security awareness training that also covers incident response training.
Contractors		
Vendors		

?		

Incident Response Testing [NIST IR-3]

To further help ensure the safety and security of [company name] critical information systems, the incident response plan is to be tested on an annual basis, with results provided to senior management as necessary. [Company name]'s incident response testing initiatives consists of the following:

[Describe your incident response testing initiatives.]

Automated Testing [NIST IR-3(1)]

[Company name] is to test the incident response capability using [Assignment: organization-defined automated mechanisms].

Coordination with Related Plans [NIST IR-3(2)]

[Company name] is to coordinate incident response testing with organizational elements responsible for related plans.

Continuous Improvement [NIST IR-3(3)]

[Company name] is to use qualitative and quantitative data from testing to: (a) Determine the effectiveness of incident response processes; (b) Continuously improve incident response processes; and (c) Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

Incident Response Preparation

The Incident Response Plan is to fit into the organization's mission that consists of ensuring the Confidentiality, Integrity, and Availability (CIA) of [company name] information systems at all times, and any incident response initiatives that do not meet or exceed such requirements, are to be re-assessed accordingly.

Additionally, as [company name] changes in size, structure, and functions – much like any organization – the Incident Response Plan is to change accordingly, ensuring it meets the demands as necessary. Furthermore, authorized personnel are to regularly measure the overall adequacy and sufficiency of the Incident Response Plan by assessing any number of defined metrics and attributes that provide meaningful insight into the plan itself.

Constant improvement of the Incident Response Plan ultimately helps ensure the ongoing safety and security of [company name] information systems. The best changes to implement are those that are learned from actual incident response measures invoked for a given incident. A "Lessons Learned" approach not only applies to why and how the incident occurred, but also to how the incident was managed.

Incident Response Capabilities

Preparation in the context of incident response requires [company name] to establish both comprehensive incident response capabilities and incident prevention initiatives. Regarding incident response capabilities, authorized personnel at [company name] are to identify, assess, and implement all necessary tools and resources that ultimately may be deemed of value during the entire incident response and reporting lifecycle. Such tools and resources are to include, but are not limited to, the following:

- **Relevant Contact Information:** Information regarding all parties involved in the overall incident response and reporting lifecycle, from internal incident response personnel to senior management, law enforcement authorities, additional external third parties, and more. Contact information is to include, but is not limited to, the following:
    - Names
    - Phone numbers
    - e-mails
    - and other information deemed necessary.
- Incident response tracking mechanisms
- Communication devices
- Relevant hardware and software tools for incident analysis
- Relevant documentation and resources for incident analysis
- Any other tools and resources deemed necessary.

Incident Response Detection

Detecting an incident requires a true commitment by all personnel to be constantly aware of their surroundings for any type of social engineering, physical or environmental threats. Additionally, detection also requires due diligence and consistency by authorized employees regarding the secure configuration and review of network and system logs, being aware of network traffic anomalies and any suspicious or disruptive network patterns or incidents. Personnel responsible for reviewing network and system logs (firewalls, routers, switches, IDS/IPS, operating systems, applications, databases, etc.) are, because of these reviews, to report any malicious, suspicious, or disruptive event immediately to the Incident Response Team.

Attack Surface

Employees are therefore to be educated and aware of the following attack surfaces against [company name]'s network:

- **External/Removable Media:** An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive.
- **Attrition:** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services, such DoS, DDoS attacks, and others.
- **Web:** An attack executed from a website or web-based application. Common security threats to websites (i.e. web application servers) can be found at OWASP (https://www.owasp.org/index.php/Main_Page)
- **Email:** An attack executed via an email message or attachment.
- **Impersonation:** An attack involving replacement of something benign with something malicious—for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
- **Improper Usage and Insider Threats:** Any incident resulting from violation of an organization's acceptable usage policies by an authorized user.
- **Loss or Theft of Equipment:** The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token.

- **Other Attacks:** All other attack surface conditions not listed above.

Precursors and Alerting Mechanisms

From an incident response perspective, "Precursors" are the various elements that provide critical information relating to a possible cyber incident. Examples of precursors include, but are not limited to, the following:

- Logging and audit trail entries
- Host-based alerts, such as File Integrity Monitoring (FIM), Anti-Virus alerts, etc.
- Network-based alerts, such as Intrusion Detection Systems (IDS), Web Application Firewalls (WAF), etc.
- Direct threats from an organization asserting they will attack a network.
- Direct threats from an employee, contractor, disgruntled associate of customers, etc.

Employees, especially those who have access to logging and alert data, are to be aware of such precursors and what indicators could potentially lead to a possible cyber incident against [company name]. This in turn requires authorized personnel to be aware of the actual sources of precursors and relevant indicators. Common sources for precursors, include, but are not limited to, the following:

- Host Based Intrusion Detection Systems (HIDS)/Intrusion Prevention Systems (HIPS), File Integrity Monitoring (FIM), Change Detection Software (CDS).
- Anti-Virus Software, Anti-Spam, Anti-Malware Software.
- Network Based Intrusion Detection Systems (NIDS)
- Audit logs from all information systems, such as logs from network devices, servers, etc.
- Information from online organizations, associations, forums, etc.

Precursors and Alerting Mechanisms

Precursors/Alerting Mechanisms	Name of Tool/Solution	Description of "Alert" Provided

Information Spillage [NIST IR-9]

Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. Corrective action is

therefore immediately required by [company name] for removing classified or sensitive data from information systems, which entails following the formalized policies and procedures listed herein.

Training [NIST IR-9(2)]
The organization is to provide information spillage response training [Assignment: organization-defined frequency].

Post-Spill Operations [NIST IR-9(3)]
The organization is to implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: [Assignment: organization-defined procedures].

Exposure to Unauthorized Personnel [NIST IR-9(4)]
The organization is to employ the following controls for personnel exposed to information not within assigned access authorizations: [Assignment: organization-defined controls].

Attack Vectors - Risks, Threats, Attacks and Related Incidents & Events
The Incident Response Plan requires all personnel (i.e., employees, contractors, vendors, etc.) to be able to identity and be aware of a wide range of security risks, threats, attacks, and related incidents & events that could impact and ultimately affect the confidentiality, integrity, and availability (CIA) of [company name]'s network and related assets. Simply stated, risks evolve into threats. Threats can turn into attacks. Attacks result in an incident against a network, which is ultimately an event.

- **Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
- **Threat:** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
- **Attack:** A type of maneuver employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by performing any number of illegal and/or unauthorized actions.
- **Incident:** An event or an occurrence that is a direct result of the relevant risks and threats.
- **Event:** An action that may have an impact on organizational operations, such as mission, capabilities, reputation, etc.

Attack Vectors - List of Risks, Threats, Attacks, and Related Incidents & Events
For [company name] to be able to adequately respond to cybersecurity occurrences, all personnel (i.e., employees, contractors, vendors, guests, etc.) need to be aware of the following risks, threats, attacks, and related incidents that can cause significant damage to organizational assets:

- **Cyber Intrusion:** The unauthorized act of spying, surveilling, and the possible theft of information and/or damage to information systems.
- **Ransomware:** A type of malicious software that essentially blocks access to the victim's data or threatens to publish or delete it until a ransom is paid
- **Malware:** An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.
- **Watering Hole:** A computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some members of the targeted group get infected. The malware used in these attacks typically collects information on the user.
- **Phishing:** The fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords, credit card numbers, Personally Identifiable Information (PII), and other data deemed sensitive and confidential.
- **Spoofing Attack:** An event in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage.
- **Web Application Development Security Risks:** These are risks associated with developing software used for web facing systems, such as e-commerce servers, publicly accessible servers that provide general content, and other forms of information that are “public” facing within the untrusted Internet. Learn more at https://www.owasp.org about such threats.
- **Denial of Service (DoS) Attack:** A cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet.
- **Distributed Denial of Service (DDoS):** A type of a type of Denial-of-Service Attack (DoS) where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.
- **Credential Reuse:** A cyber incident whereby account credentials are leaked from one website, and because users often use the exact same or similar passwords on multiple websites, those accounts are then also compromised.
- **Deliberate, Unauthorized Access Attempts:** Abuse by an individual to gain access to a system by continuing to enter a username and password until they are effectively locked out or ultimately denied.
- **Session Hijacking and Man-in-the-Middle (MITM) Attacks:** The exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. It is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has relevance to web developers, as the HTTP cookies used to maintain a session on many websites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. Simply

stated, any attack that involves the exploitation of a session between devices is session hijacking, with the "session" being a connection between devices in which there is state.

- **Hacktivism:** The subversive use of computers and computer networks to promote a political agenda
- **Drone Jacking:** The hijacking of a drone, either by physically capturing the device or by compromising its navigation system.
- **Social Engineering:** The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
- **Insider Threats:** A malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.
- **Acceptable Use Violations:** Violating an organization's usage rights to information systems.
- **Loss or Theft of Assets:** Assets (such as physical assets, along with data and information) that are either physically or electronically lost or stolen.
- **Loss or Theft of Sensitive Data:** The loss (i.e., theft or unauthorized use) of data, which includes, but is not limited to the following: Protected Health Information (PHI), Personally Identifiable Information (PII), Personally Identifiable Financial Information (PIFI), cardholder data, and other types of data deemed personal/confidential, etc.
- **Rogue Software:** A form of malicious software and Internet fraud that misleads users into believing there is a virus on their computer and manipulates them into paying money for a fake malware removal tool (that introduces malware to the computer). It is a form of scareware that manipulates users through fear, and a form of ransomware.
- **Drive-by-Downloads:** The unintentional download of a virus or malicious software (malware) onto your system. A drive-by attack will usually take advantage of (or "exploit") a browser, app, or operating system that is out of date and has a security flaw.
- **Malvertising:** The use of online advertising to spread malware by injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.
- **Advanced Persistent Threats:** A network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization.
- **Other:** Any other risk, threat, attack, and related incident not discussed in the above listed descriptions.

[Company Name] Data Governance Program & Charter

Official Policy Title:	
Responsible Party:	
Approval Party:	
Effective Date:	
Last Update:	
Version Number:	
Policy Framework:	**Developed in accordance with NIST Special Publication (SP) 800 Series - https://csrc.nist.gov/publications/sp800**
Mapping	**(1). NIST SP 800-53, rev. 5 [NIST PM-23]**

Introduction

The Data Governance Program & Charter referenced within this document defines the security measures to be implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, the Data Governance Program & Charter is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Data Governance Program & Charter is to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

In terms of defining data governance, [company name] embraces the following definition as its driving force for implementing the Data Governance Program & Charter.

An organizational approach to data and information management that is formalized as a set of policies and procedures that encompass the full life cycle of data, from acquisition to use to disposal. This includes establishing decision-making authority, policies, procedures, and standards regarding data security and privacy protection, data inventories, content and records management, data quality control, data access, data security and risk management, data sharing and dissemination, as well as ongoing compliance monitoring of all the above-mentioned activities.

Mission

The Data Governance Program & Charter seeks to create the most conducive environment for purposes of supporting organization-wide data-driven decision-making. As such, the Data Governance Program & Charter seeks to identify data that currently exists, data that needs to exist in the future, define roles and responsibilities related to the ownership and management of that data, and to also assign accountability of those responsibilities to specific groups or individuals within the organization.

Goals and Objectives

The Data Governance Program & Charter seeks to improve data quality all throughout the organization, ultimately, maximizing data use for achieving all stated and desired goals. To achieve such goals, [company name] will employ all necessary measures relating to 'People, Processes, and Technology'. These three key areas, when working together, will help ensure [company name]'s data governance policies, procedures, programs, and plans are implemented and successfully carried out. Furthermore, such measures ultimately drive the measures that ensure privacy and compliance in an organization's enterprise data management.

People: People (senior leadership and all relevant stakeholders) are without question the most important aspect of the Data Governance Program & Charter. As such, it is incumbent upon [company name] that the Data Governance Program & Charter embraces and advances the following measures for good data governance:

- Champion the values - and implications - of data governance and the importance of a culture that clearly embraces use of data in achieving organization goals and making positive change through continuous improvement in all areas.
- Make aware of the importance of sponsoring analytics efforts, advocating for a structured approach to analytics, and allocating resources for analytics efforts.
- Define, agree, and communicate, and advance the roles and responsibilities of data stewards.
- Identify and establish cross-functional teams to drive the organization's data governance practices.
- Ensure that relevant stakeholders are kept fully informed of the data governance changes and that they champion such changes throughout the organization.
- At all times, drive organizational and behavioral change as it relates to the use of data.

Processes: Processes are the series of actions and related steps taken to achieve a desired end. As such, it is incumbent upon [company name] that the Data Governance Program & Charter embraces and advances the following measures for good data governance:

- Establish and set realistic and achievable priorities for data governance activities.
- Implement measures to successfully identify and track realization of benefit opportunities arising from the provision and use of better-quality information.
- Empower stakeholders with guidance, standards and unwavering support that allows them to develop commonly used data definitions for all shared data.

- Develop and implement comprehensive, quality data quality policies, procedures, processes, and quality measures.
- Support all initiatives relating to growing regulatory compliance mandates.
- Implement a 'Security First' mindset into all aspects of data governance.
- Work in a collaborative manner with all relevant stakeholders by designing and implementing processes for good data governance.

Technology: Technology is the application of knowledge for achieving practical goals in a reproducible way. As such, it is incumbent upon [company name] that the Data Governance Program & Charter embraces and advances the following measures for good data governance:

- Implement technology tools and solutions that foster data quality and reporting.
- Implement security tools and solutions that promote a 'Security First' mindset.
- Seek any additional technology resources that will better enable the organization's overall data governance practices.

Guiding Principles

The following guiding principles are a critical component of [company name]'s Data Governance Program & Charter:

- **Clarity:** This implies that the organization has a clear mission, with stated policies, procedures, processes, and programs in place.
- **Assessments:** This implies that the organization is to consistently measure the progress against the stated goals, and ultimately, determine how to improve upon such measures.
- **Consistency:** This implies that all measures undertaken are applied with regularity.
- **Leadership:** This implies that everyone has roles and responsibilities for adhering to data governance, which in turn ultimately helps ensure the Confidentiality, Integrity, and Availability (CIA) of the organization' data.
- **Accountability:** This implies that for all data actions, there are consequences, both good and bad, thus, the organization is to make aware of the consequences of good data actions, but also those that can adversely affect the organization.
- **Agility:** This implies that the organization should be ready to adjust and accommodate changes to the organization's data with regards to it being collected, used, shared & disclosed, stored, protected, retained, and disposed.

Application of Metrics

The Data Governance Program & Charter is to establish, implement, and continuously monitor the following categories with the application of both qualitative and quantitative metrics for measuring progress:

- **Accessibility:** Ensure that only authorized users have access to data for performing their respective roles and responsibilities. Specifically, such access is to be granted with the application of Role Based Access Control (RBAC).
- **Awareness & Training:** Ensure that all users of data have undertaken general security awareness training, and as needed, awareness & training relating to data governance practices.
- **Accuracy:** Ensure that measures are in place to promote data accuracy in all aspects of using data within the organization.
- **Collection:** Ensure that measures are in place to collect data safely and securely, and that such collection of data is legally allowed.
- **Completeness:** Ensure that measures are in place that data is complete in terms of all activities relating to data being collected, used, shared & disclosed, stored, protected, retained, and disposed.
- **Compliance:** Ensure that measures are in place to identify, address, and comply with all stated regulatory compliance laws, regulations, etc.
- **Consistency:** Ensure that measures are in place that data is consistent in terms of all activities relating to data being collected, used, shared & disclosed, stored, protected, retained, and disposed.
- **Disposal:** Ensure that measures are in place to appropriately dispose of data - both hard-copy and electronic data - as necessary.
- **Efficiency:** Ensure that measures are in place that data is consistent in terms of all activities relating to data being collected, used, shared & disclosed, stored, protected, retained, and disposed.
- **Security:** Ensure that measures are in place to promote the safety and security of data in terms of all activities relating to data being collected, used, shared & disclosed, stored, protected, retained, and disposed.
- **Sharing:** Ensure that measures are in place for sharing data with trusted organizations, those that have a rightful need to have access to data.
- **User Acceptance and Satisfaction:** Ensure that measures are in place to assess the overall usability, acceptance, and satisfaction of data.

Privacy by Design for Good Data Governance

A key component of [company name]'s Data Governance Program & Charter is to implement *Privacy by Design:* Privacy by Design, is a concept that calls for ensuring privacy is built into every aspect of an organization, an integral element that should be incorporated into every standard, protocol, and process, and that includes data regarding [company name]'s Data Governance Program & Charter. The foundational principles of Privacy by Design consist of the following seven (7) categories:

1. Proactive not Reactive; Preventative not Remedial: A clear commitment, at the highest levels, to set and enforce high standards of privacy. A privacy commitment that is demonstrably shared throughout by user communities and stakeholders. Established methods to recognize poor privacy designs, anticipate poor privacy practices and outcomes, and correct any negative impacts, well before they occur in proactive, systematic, and innovative ways.

2. Privacy as the Default Setting: Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data is automatically protected in any given IT system or business practice. If an individual does nothing, their privacy remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.
3. Privacy Embedded into Design: Privacy must be embedded into technologies, operations, and information architectures in a holistic, integrative, and creative way. Holistic, because additional, broader contexts must always be considered. Integrative, because all stakeholders and interests should be consulted. Creative, because embedding privacy sometimes means re-inventing existing choices because the alternatives are unacceptable.
4. Full Functionality – Positive-Sum, not Zero-Sum: Satisfying all an organization's legitimate objectives − not only its privacy goals, thus, real, practical results and beneficial outcomes to be achieved for multiple parties.
5. End-to-End Security – Full Lifecycle Protection: Strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.
6. Visibility and Transparency – Keep it Open: Remain visible and transparent, to both users and providers alike. Remember, trust but verify.
7. Respect for User Privacy – Keep it User-Centric: Keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user centric.

Data Management Lifecycle

A key component of [company name]'s Data Governance Program & Charter is to document the organization's data management lifecycle regarding how data is collected, used, shared & disclosed, stored, protected, retained, and disposed.

Data Collection: Data is collected through the following measures:

Data Type	Collection Method	Description
	Data collected via HTTPS via port 443	
	Data downloaded from SFTP site from clients	

ABOUT ARLINGTON SECURITY PORTAL

What is ASP?:

Arlington Security Portal (ASP) is an online repository of world-class, industry leading security and privacy policies & procedures, programs, plans – and other highly essential documents & templates developed specifically on NIST SP 800-53, Revision 5.

Features:

Easy-to-use and edit MS Word documents providing complete coverage for all required policies, procedures, programs, and plans for NIST SP 800-53, Revision 5.

Benefits:

Saves federal contractors an incredible amount of time and money with best-in-class security and privacy documents that map directly to the twenty (20) NIST SP 800-53, Revision 5 control families.

Advantages:

Industry first, one-stop portal for all your NIST SP 800-53, Revision 5 documents that are comprehensive, yet easy-to-use and implement security and privacy policies & procedures, programs, and plans available anywhere.

WE ARE ARLINGTON

A team of innovative, solution-oriented, highly agile, and well-versed professionals with decades of experience in working with America's defense industry. From emerging cybersecurity regulations to helping our clients solve complex security & compliance solutions – and so much more – you can trust Arlington, the firm that's Dedicated to Defense®.

Our professionals are seasoned veterans in the DoD sector, men and women who've walked the halls of the Pentagon and many other agencies within America's intelligence apparatus.

Why Arlington?

Today's Defense Industrial Base (DIB) is bigger, more complex, and more vulnerable to attacks – than ever before. From insider threats to malicious hackers thousands of miles away, America's defense industry is under assault from all fronts.

With more than 400,000 + organizations comprising America's DIB, this vast and still growing industry is a core component of protecting the very fabric of our critical infrastructure.

Without America's defense contractors in full play, our country lies vulnerable to any number of attacks from nefarious forces. In recent years, a wave of standards and regulations have inundated defense contractors, forcing organizations to spend considerable time, money, and resources on meeting today's demanding Department of Defense (DoD) compliance requirements.

It's time for defense contractors to get serious about protecting their information systems, and it's time for a new type of organization to assist.

ARLINGTON
DEDICATED TO DEFENSE

CORPORATE HEADQUARTERS

(855) 222-9592

info@arlingtonintel.com

www.arlingtonintel.com

2300 Wilson Blvd., Suite 700
Arlington, VA 22201