[Company Name Or Logo]	
Title: Data Security	**P&P #: [Insert Here]**
Approval Date: [Date]	**Review:**
Effective Date: [Date]	**Information Technology**

Purpose

The document lays out the policies and procedures of how to secure and protect data to maintain confidentiality and integrity. To guarantee that IT resources and information systems are protected via system integrity monitoring, which includes malware, application and source code defects, industry-supplied alerts, and the correction of found or revealed integrity concerns.

Scope

This policy applies to all employees and other members of the workforce (paid, volunteer or contractor) working in all facilities under the organization's ownership.

Definitions

Integrity – guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Denial-of-service (DoS) - The prevention of authorized access to resources or the delaying of time-critical operations.

Policy

Our Security Officer and/or Information System Owner will implement policies and procedures for protecting and responding to suspected or known date leaks. Data should be maintained for its integrity and is available in any given situations such as DoS attacks, documenting date security incidents and their outcomes.

Procedures

Security Officer and/or Information System Owner shall:

- Update and maintain the policy document to reflect its current data security focus and notify the appropriate individuals so that everyone is on the same page.
- Ensure that all data-at-rest is protected by adhering to the company's policies and procedures.
- Follow and maintain availability of data by allocating appropriate storage capacity along with backup power supply in case of emergency.

PURDUE UNIVERSITY
cyberTAP
This template is provided by the Purdue University Cyber Technical Assistance Program.
This template may be used, distributed, and shared without restriction. The watermark may be removed or replaced. White labeling this template is permitted.
For questions contact us via our website: https://cyber.tap.purdue.edu

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

- Monitor and enforce controls to prevent and protect data leaks.

PR.DS-P1: Data-at-rest are protected
NIST 800-53 Revision 5

1. All media and information should be protected by the organization and individuals that have access and utilization of:
    a. The Data Owner and Information System Owner guarantee that only authorized users have access to digital material for all information systems.
2. For all moderate and high-risk information systems, the Data Owner and Information System Owner ensure that:
    a. The distribution constraints, handling caveats, and appropriate data categorization labels (if any) of information system digital media are indicated.
    b. All digital media is physically protected and stored in access-restricted, environmentally acceptable locations.
    c. Data stored on secondary storage devices (devices that retain copies of data stored on primary data storage devices) must be encrypted.
    d. Information system media is protected until it is destroyed or sanitized using approved equipment, techniques, and procedures.
    e. During transfer outside of regulated zones, accountability for information system media is maintained.
    f. Activities associated with the transport of information system media are documented.
3. For high-risk information systems, the Data Owner and Information System Owner ensure that media sanitization and disposal actions are reviewed, approved, tracked, documented, and verified.
4. For high-risk information systems, the Data Owner and Information System Owner ensure that testing to sanitization equipment and procedures to verify that the intended sanitization is being achieved occurs annually.

PR.DS-P4: Adequate capacity to ensure availability is maintained
NIST Special Publication 800-53 Revision 5

1. The Security Officer and/or Information System Owner is responsible in ensuring availability is maintained by implementing the following measures:
    a. Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.
    b. Develop a contingency plan for the system that:
        i. Identifies essential mission and business functions and associated contingency requirements.
        ii. Provides recovery objectives, restoration priorities, and metrics.
        iii. Addresses contingency roles, responsibilities, assigned individuals with contact information

PURDUE UNIVERSITY
CyberTAP
This template is provided by the Purdue University Cyber Technical Assistance Program.
This template may be used, distributed, and shared without restriction. The watermark may be removed or replaced. White labeling this template is permitted.
For questions contact us via our website: https://cybertap.purdue.edu

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

c. Provide an uninterruptible power supply to facilitate an orderly shutdown of the system and transition of the system to long-term alternate power in the event of a primary power source loss
d. The information system restricts the ability of users to launch denial of service attacks against other information systems or networks
e. The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

PR.DS-P5: Protections against data leaks are implemented
NIST Special Publication 800-53 Revision 5

1. The Security Officer and/or Information System Owner should maintain data security and prevent data leaks by:
    a. Enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information control.
    b. Define system access authorizations to support separation of duties.
    c. Employ the principle of least privilege, allowing only authorized accesses for users or processes acting on behalf of users that are necessary to accomplish assigned organizational tasks.
    d. Protect the system from information leakage due to electromagnetic signals emanations.
    e. Develop and document access agreements for organizational systems.
    f. Review and update the access agreements quarterly.
    g. Verify that individuals requiring access to organizational information and systems:
        i. Sign appropriate access agreements prior to being granted access
    h. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.
    i. Implement subnetworks for publicly accessible system components that are logically separated from internal organizational networks.
    j. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

PR.DS-P7: The development and testing environment(s) are separate from the production environment
NIST Special Publication 800-53 Revision 5

1. Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.
2. Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

PURDUE UNIVERSITY CyberTAP
This template is provided by the Purdue University Cyber Technical Assistance Program.
This template may be used, distributed, and shared without restriction. The watermark may be removed or replaced. White labeling this template is permitted.
For questions contact us via our website: https://cyber.tap.purdue.edu

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity
NIST Special Publication 800-53 Revision 5

1. This policy is applicable to all departments and users of IT resources and assets.
    a. Identify, report, and correct information system flaws.
    b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
    c. Install security-relevant software and firmware updates within 3 days of the release of the updates.
    d. Incorporate flaw remediation into the configuration management process.
    e. Employ automated mechanisms weekly to determine the state of information system components about flaw remediation.

Violations: Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

Attachments: None

Related Policies:

PURDUE UNIVERSITY
cyberTAP
This template is provided by the Purdue University Cyber Technical Assistance Program.
This template may be used, distributed, and shared without restriction. The watermark may be removed or replaced. White labeling this template is permitted.
For questions contact us via our website:
https://cyber.tap.purdue.edu

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.