# IS-17 Data Integrity Policy

**17.1 Data Integrity Policy**

<COMPANY NAME> takes data integrity very seriously. As stewards and partners of <COMPANY NAME> Customers, we strive to assure data is protected from unauthorized access and that it is available when needed. The following policies drive many of our procedures and technical settings in support of the <COMPANY NAME> mission of data protection.

Production systems that create, receive, store, or transmit Customer data (hereafter "Production Systems") must follow the guidelines described in this section.

**17.2 Disabling Non-Essential Services**

1. All Production Systems must disable services that are not required to achieve the business purpose or function of the system.

**17.3 Monitoring Log-in Attempts**

1. All access to Production Systems must be logged. This is done following the <COMPANY NAME> Auditing Policy.

**17.4 Prevention of Malware on Production Systems**

1. All Production Systems must have anti-malware tools running, and set to scan system every 2 hours and at reboot to assure no malware is present. Detected malware is evaluated and removed.
2. Virus scanning software is run on all Production Systems for anti-virus protection.
	* Hosts are scanned daily for malicious binaries in critical system paths.
	* The malware signature database is checked hourly and automatically updated if new signatures are available.
	* Logs of virus scans are maintained according to the requirements outlined in 8.6-audit-log-security-controls-and-backup.
3. All Production Systems are to only be used for <COMPANY NAME> business needs.

**17.5 Patch Management**

1. Software patches and updates will be applied to all systems in a timely manner. In the case of routine updates, they will be applied after thorough testing. In the case of updates to correct known vulnerabilities, priority will be given to testing to speed the time to production. Critical security patches are applied within 30 days from testing and all security patches are applied within 90 days after testing.

2. Administrators subscribe to mailing lists to ensure that they are using current versions of all <COMPANY NAME>-managed software on Production Systems.

**17.6 Intrusion Detection and Vulnerability Scanning**

1. Production systems are monitored using IDS systems. Suspicious activity is logged and alerts are generated.
	* file system integrity is monitored and sends real time alerts when suspicious changes are made to the file system.
	* Automatic monitoring is done to identify patterns that might signify the lack of availability of certain services and systems (DoS attacks).
	* <COMPANY NAME> firewalls monitor all incoming traffic to detect potential denial-of-service attacks. Suspected attack sources are blocked automatically. Additionally, our hosting provider actively monitors its network to detect denial-of-service attacks.
	* All new firewall rules and configuration changes are tested before being pushed into production. All firewall and router rules are reviewed at least annually.
2. Vulnerability scanning of Production Systems must occur on a predetermined, regular basis, no less than annually. Currently it is weekly. Scans are reviewed by Security Officer, with defined steps for risk mitigation, and retained for future reference.

**17.7 Production System Security**

1. System, network, and server security is managed and maintained by the Security Officer in conjunction with the Dev Ops team.
2. Up-to-date system lists and architecture diagrams are kept for all production environments.
3. Access to Production Systems is controlled using centralized tools and two-factor authentication.

**17.8 Production Data Security**

1. Reduce the risk of compromise of Production Data.
2. Implement and/or review controls designed to protect Production Data from improper alteration or destruction.
3. Ensure that confidential data is stored in a manner that supports user access logs and automated monitoring for potential security incidents.
4. Ensure <COMPANY NAME> Customer Production Data is segmented and only accessible to Customers authorized to access data.
5. All Production Data at rest is stored on encrypted volumes using encryption keys managed by <COMPANY NAME>.
6. Volume encryption keys and machines that generate volume encryption keys are protected from unauthorized access. Volume encryption key material is protected with access controls such that the key material is only accessible by privileged accounts.
7. Encrypted volumes use AES encryption with a minimum of 256-bit keys, or keys and ciphers of equivalent or higher cryptographic strength.

**17.9 Transmission Security**

1. All data transmission is encrypted end to end using encryption keys managed by <COMPANY NAME>. Encryption is not terminated at the network end point, and is carried through to the application.
2. Transmission encryption keys and machines that generate keys are protected from unauthorized access. Transmission encryption key material is protected with access controls such that the key material is only accessible by privileged accounts.
3. Transmission encryption keys use a minimum of 4096-bit RSA keys, or keys and ciphers of equivalent or higher cryptographic strength (e.g., 256-bit AES session keys in the case of IPsec encryption).
4. Transmission encryption keys are limited to use for one year and then must be regenerated.
5. In the case of <COMPANY NAME> provided APIs, provide mechanisms to assure person sending or receiving data is authorized to send and save data.
6. System logs of all transmissions of Production Data access. These logs must be available for audit.

**Purpose**

The purpose of this policy is to ensure that the confidentiality, integrity and availability of data that the company stores, processes and transmits are protected according to applicable laws, regulations and standards.

**Scope**

This policy applies to systems that receive, store, or transmit confidential or critical information. All users of the company’s information systems are responsible for complying with and understanding this policy. This includes (but is not limited to) employees, consultants, contractors, vendors, business partners and temporary staff.

**Applicable Standards**

Applicable Standards from the HITRUST Common Security Framework

* 09.ab - Monitoring System Use
* 06.e - Prevention of Misuse of Information
* 10.b – Input Data Validation
* 10.h - Control of Operational Software

Applicable Standards from the HIPAA Security Rule

* 164.308(a)(8) - HIPAA Security Rule Evaluation
* 164.312(b) - Audit Controls

# **Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description of changes** |
|  |  | **Initial creation** |
|  |  |  |
|  |  |  |