



IT Security Policy

Version 1.1



SYSREFORMS
INTERNATIONAL

IT Security Policy

Version: 1.1

Dated: 29 August 2024

Updated by: Ms. Fazila Kausar, Information Security Officer

Version Notes: This version includes enhanced monitoring, risk management, regulatory compliance, and accountability, further aligning the ITSP with GDPR and ISO 27001 best practices. It is now positioned as a comprehensive, proactive, and compliant security policy.

1. Awareness and Training

All employees are required to complete data security and privacy training upon onboarding, covering GDPR and ISO 27001 requirements. Periodic training is conducted on emerging threats, data protection best practices, and organizational security policies. Training completion is tracked, and any employee failing to comply may face disciplinary action. Annual refresher training is mandatory for all staff.

2. Personnel Practices

Employees sign a confidentiality and security acknowledgment form to confirm understanding and commitment to GDPR and ISO 27001 standards. Access rights are promptly revoked upon off-boarding, with a final exit interview to ensure no proprietary information is retained. Role-based access reviews are conducted semi-annually to align access privileges with current job responsibilities.

3. Administrative Roles and Responsibilities

System administrators follow ISO 27001-compliant protocols, maintaining systems, addressing technical issues, and documenting all administrative actions. Roles with elevated privileges are reviewed quarterly to ensure that only authorized personnel have necessary access, reducing unnecessary privilege exposure.

4. Network and Telecommunications Security

Network infrastructure is segmented into zones based on functionality, with encrypted channels (AES-256, SSL/TLS) for all data transfers involving personal or sensitive data. Regular access reviews and security audits, conducted quarterly, ensure ongoing network integrity and compliance with GDPR and ISO 27001 standards.

5. Incident Detection and Response Plan

A comprehensive incident response plan is in place to address security incidents, data breaches, and vulnerabilities. The response plan includes:

- **Risk Analysis:** IT Security Coordinator is responsible to conduct a quarterly or as and when required risk analysis and recommend/implement mitigation measures.
- **Detection and Reporting:** All employees are trained to identify and report security issues within 24 hours.
- **Breach Notification:** Any breach involving personal data will be reported to relevant authorities within 72 hours, in compliance with GDPR.
- **Documentation and Analysis:** All incidents are documented, with a root cause analysis conducted to prevent recurrence.

- **Post-Incident Review:** A formal review process improves incident response procedures.

6. **Malicious Code Control (Antivirus)**

Anti-malware and antivirus solutions are installed on all endpoints and servers, with real-time monitoring and automatic updates. Regular scanning for malware is scheduled weekly, with reports generated for review. Any identified malware incidents are documented and escalated as needed.

7. **Portable Computing Security**

Portable devices storing or accessing confidential information must be encrypted and secured. Unauthorized data storage on portable devices is strictly prohibited, and all devices must meet the company's remote access standards, including VPN and multi-factor authentication (MFA) for secure external network access.

8. **Logical and System Access**

Access controls are enforced in line with GDPR's data protection and ISO 27001's access control standards. Passwords must meet complexity requirements, include at least 12 characters, and be changed every 90 days. Multi-factor authentication (MFA) is mandatory for accessing sensitive systems and is regularly reviewed.

9. **Physical Access Control**

Critical components are housed in an ISO/IEC 27001-certified facility, with strict access control. Physical access is restricted to authorized personnel using biometric verification, and visitor logs are maintained and audited quarterly. Surveillance, environmental monitoring, and regular audits protect against unauthorized access.

10. **At-Rest and in-Transit Data Protection**

For **at-rest** and **in-transit** data protection, SysReforms International implements robust security measures to ensure data confidentiality, integrity, and availability. These measures collectively will protect data from unauthorized access, interception, and tampering, ensuring compliance with industry security standards. These include:

10.1 **At-Rest Data Protection**

10.1.1 **Encryption**

- Data is encrypted using AES-256 encryption to prevent unauthorized access.
- Database encryption (TDE - Transparent Data Encryption) is applied where supported.

10.1.2 **Access Control**

- Role-based access control (RBAC) restricts data access to authorized users.
- Multi-factor authentication (MFA) ensures enhanced security.

10.1.3 **Data Masking & Tokenization**

- Sensitive data is masked or tokenized to protect against leaks and breaches.

10.1.4 **Backup Security**

- Encrypted, redundant backups are maintained for disaster recovery.
- Secure offsite storage for backup data to prevent unauthorized access.

10.1.5 **Audit Logging & Monitoring**

- Continuous monitoring of access logs and audit trails to detect anomalies.
- Security Information and Event Management (SIEM) tools for real-time threat detection.

10.2 **In-Transit Data Protection**

10.2.1 **TLS/SSL Encryption**

- All data transmissions use TLS 1.2 or higher to ensure secure communication.

- Secure HTTPS connections for web applications and API communications.

10.2.2 Secure Tunneling:

- VPNs and SSH tunneling for secure remote access.
- Encrypted connections for database queries and remote administrative tasks.

10.2.3 HSTS (HTTP Strict Transport Security):

- Enforces HTTPS connections to prevent downgrade attacks and man-in-the-middle attacks.

10.2.4 Certificate Pinning:

- Prevents attackers from impersonating trusted servers using fake SSL certificates.

10.2.5 Integrity Verification:

- Message authentication codes (MAC) or digital signatures ensure data integrity during transmission.

11. Firewall Management

A “deny all” approach is enforced for firewall management, allowing only necessary and pre-approved services through. Firewall configurations are reviewed monthly, with change logs maintained to document any adjustments to security settings.

12. Third-Party Services and Vendor Risk Management

Before engaging with any third-party service, a detailed risk assessment is conducted. This assessment evaluates data protection compliance, contractual obligations, and security posture. Ongoing monitoring and annual reassessments ensure continued adherence to SysReforms’ security policies. Data processing agreements (DPAs) are mandatory for all third-party vendors handling personal data.

13. Software Licensing and Usage

All software use is monitored, recorded, and subject to periodic audits to prevent unauthorized or unlicensed software installation. Installation of software without proper licensing is prohibited, protecting against potential security risks and regulatory non-compliance.

14. Auditing, Logging, and Monitoring

System and application data is logged in compliance with GDPR’s requirements for traceability and ISO 27001 standards. Logs are securely stored, accessible only to authorized personnel, and reviewed annually to identify any suspicious activity or potential security risks.

15. Remote Work and Access Security

Remote work is restricted to authorized personnel who follow strict security protocols, including VPN, encryption, and MFA. Personal use of company-provided equipment is prohibited. Regular security checks on remote connections help ensure compliance with GDPR and ISO 27001 standards.

16. Data Classification, Confidentiality, Integrity, and Availability

Data is classified into levels of sensitivity (e.g., Confidential, Restricted, Public). Access to confidential data is limited to personnel with a need-to-know basis and documented approval. All data access follows GDPR’s confidentiality, integrity, and availability principles, managed across the data lifecycle.

17. Data Loss Prevention (DLP)

DLP measures are in place to prevent unauthorized data transfers and monitor high-risk data flows, such as USB use and external cloud storage. Data access and transfers

are logged and regularly audited, ensuring that data handling complies with GDPR and internal policies.

18. Patch and System Update Management

A proactive patch management program ensures that all software is regularly updated to minimize security vulnerabilities. Updates are applied within 30 days of release for standard patches, and immediately for critical patches, following a testing phase to prevent operational disruption. Test system and security patches before implementing them in the production environment will be ensured.

19. Compliance with Privacy Regulations

SysReforms adheres to GDPR, ISO 27001, and other relevant data protection laws. Regular audits and policy reviews ensure continued compliance, with employee training on regulatory updates to meet evolving privacy requirements.

20. Data Backup and Disaster Recovery

Critical data, including critical data, is backed up every 15 minutes across multiple locations. Regular disaster recovery testing is conducted annually to verify the effectiveness of the data backup and recovery process, meeting ISO 27001 standards for business continuity.

21. System Hardening

A system hardening process removes all unnecessary software, services, and default usernames from core systems to reduce vulnerabilities. Regular vulnerability assessments ensure compliance with GDPR and ISO 27001, protecting against backdoor access.

22. Policy Compliance and Enforcement

Compliance with this policy, GDPR, and ISO 27001 is mandatory for all employees. Violations will result in corrective actions determined by the Information Security Officer. Compliance audits occur annually to identify potential improvements and gaps.

23. Policy Review and Update Cycle

This policy is reviewed annually or as needed to address regulatory changes, emerging security threats, and evolving business needs. A compliance officer, in consultation with relevant stakeholders, oversees each review to ensure alignment with GDPR, ISO 27001, and internal requirements.

24. Metrics and Accountability

Metrics such as incident response time, audit findings, and data access anomalies are tracked to assess the policy's effectiveness. Responsibility for each section is assigned to relevant departments, ensuring accountability and ongoing policy adherence.

25. Procedure for Decommissioning Old Devices Containing Customer Data

To ensure secure decommissioning of old devices that may have contained customer data, SysReforms International follows a **structured, compliant, and risk-mitigating** process.

25.1.1 Assessment & Inventory Check

- Identify and catalog all devices scheduled for decommissioning.
- Check if the device contains any **sensitive customer data** or **confidential information**.
- Verify data classification and retention policies before proceeding.

25.1.2 Secure Data Backup & Migration

- **Backup essential data** to a secure and compliant storage location.
- Verify successful migration and data integrity before proceeding with data removal.

25.1.3 Data Sanitization (Wiping & Destruction)

- **Logical Data Wiping:**
 - Use certified data erasure tools such as **Blancco, DBAN (Darik's Boot and Nuke), or built-in OS-level secure erase commands.**
 - Ensure data is **overwritten multiple times (DoD 5220.22-M, NIST 800-88 standard).**
- **Cryptographic Erasure (for Encrypted Drives):**
 - Delete encryption keys to render the data permanently unreadable.
- **Physical Destruction (if required):**
 - Shredding, degaussing, or incineration for HDDs, SSDs, USBs, and tapes.
 - Certified disposal partners are engaged for environmentally safe destruction.

25.1.4 Verification & Documentation

- Conduct a final verification to confirm successful data erasure.
- Maintain logs of the decommissioning process, including:
 - Device serial numbers
 - Date of erasure/destruction
 - Method used
 - Responsible personnel
- Obtain **certificate of destruction** if using third-party disposal services.

25.1.5 Disposal or Repurposing

- **If repurposed internally:** Reinstall the OS and apply security patches before reuse.
- **If donated/recycled:** Ensure complete erasure and compliance with e-waste disposal regulations.
- **If disposed:** Use certified electronic waste (e-waste) disposal vendors to ensure environmentally safe destruction.

25.1.6 Compliance & Audit Readiness

- Ensure adherence to **ISO 27001, GDPR, NIST, and other applicable regulations.**
- Conduct periodic audits to verify compliance with data disposal policies.

SysReforms International guarantees **customer data protection, regulatory compliance, and secure device decommissioning** while minimizing risks of data breaches.

26. Confirmation of Adherence

All employees of SysReforms are required to formally acknowledge adherence to the security policy on an annual basis. IT Security Coordinator to ensure compliance.

Glossary

- **Access Control:** Mechanisms and policies that restrict access to data, systems, and resources based on user roles and permissions, ensuring that only authorized individuals can access sensitive information.
- **AES (Advanced Encryption Standard):** A widely used encryption standard for securing data, offering different key sizes (128, 192, or 256 bits) for varying levels of protection.
- **Anti-Malware:** Software designed to detect, prevent, and remove malicious software such as viruses, worms, and trojans from a system.
- **Audit:** A systematic review of systems, processes, and logs to ensure compliance with security policies, standards, and regulatory requirements.
- **Backup:** The process of copying data to a separate location to prevent loss in case of system failure, accidental deletion, or other incidents.
- **Biometric Verification:** A method of verifying an individual's identity through unique biological traits, such as fingerprints or retinal scans, often used for physical access control.
- **Confidentiality:** The principle of protecting information so that only authorized individuals have access, especially when dealing with sensitive or personal data.
- **Data Classification:** The process of categorizing data by its sensitivity and criticality to help apply appropriate protection levels based on regulatory and organizational requirements.
- **Data Encryption:** The use of cryptographic techniques to encode data, making it unreadable to unauthorized users. It is used to protect data in transit and at rest.
- **Data Loss Prevention (DLP):** Tools and strategies that help prevent unauthorized access, transfer, or leakage of sensitive data outside the organization.
- **Data Processing Agreement (DPA):** A legally binding contract that outlines the terms for data handling by a third-party service provider, especially in compliance with GDPR.
- **Data Retention:** Policies and practices defining how long data should be kept before being securely deleted, based on its relevance and regulatory requirements.
- **Disaster Recovery Plan (DRP):** A documented, structured approach to responding to unplanned incidents that disrupt IT systems, ensuring data and operational continuity.
- **Encryption:** The process of converting data into a coded format to prevent unauthorized access, often required for sensitive or personal data under GDPR.
- **Firewall:** A security device or software that monitors and controls incoming and outgoing network traffic based on predefined security rules.
- **GDPR (General Data Protection Regulation):** A regulation by the European Union that governs data protection and privacy for all individuals within the EU, emphasizing individuals' rights to data privacy and security.
- **Incident Response Plan:** A set of instructions and procedures that outline how to detect, respond to, and recover from security incidents and data breaches.
- **Information Security Management System (ISMS):** A framework of policies and procedures that manage and protect an organization's information assets, aligning with ISO 27001 standards.
- **ISO 27001:** An international standard for managing information security, defining best practices and controls to secure information assets within an organization.

- **Multi-Factor Authentication (MFA):** An authentication method that requires multiple forms of verification to access a system, such as a password and a security code, enhancing security by reducing unauthorized access.
- **Need-to-Know Basis:** A security principle that grants access to data or resources only to individuals who need it to perform their specific job functions.
- **Patch Management:** The process of applying updates or patches to software and systems to fix vulnerabilities and improve security, often scheduled regularly.
- **Personal Data:** Any information that can identify an individual, directly or indirectly, such as name, contact details, location, or online identifiers, protected under GDPR.
- **Privacy by Design:** The practice of embedding data protection and privacy into the design of products, systems, and processes, as required by GDPR.
- **Risk Assessment:** The process of identifying, evaluating, and prioritizing risks to information assets, often guiding the selection of security controls.
- **Role-Based Access Control (RBAC):** A method of restricting system access based on user roles, assigning permissions based on the user's job functions.
- **Security Audit:** A review process that assesses an organization's security policies, practices, and infrastructure to ensure compliance with regulatory standards and internal policies.
- **System Hardening:** Strengthening the security of a system by reducing vulnerabilities, such as disabling unnecessary services, accounts, or software.
- **Virtual Private Network (VPN):** A secure connection that encrypts data transferred over the internet, commonly used to secure remote access to an organization's internal network.
- **Vulnerability Assessment:** The process of identifying, quantifying, and prioritizing security weaknesses in a system to reduce risk of unauthorized access or attack.

CONTACT US



Office # 15, Hamadan Heights,
Islamabad Expressway,
Phase 5, Ghauri Town,
Islamabad, Pakistan



92-51-8743328



92-333-1512232; 92-322-5121234



info@sysreforms.com



www.sysreforms.com