Noureddine Kanzari

ISO/IEC 27002:2022

Master the Essentials of Information Security Controls

Your Poth to Achieving ISO/IEC 27001 Certification

Learn How to Avoid Miner and Major Non-Conformities

Part 3

Learn by Doing: Practical Guide

About the author

Noureddine Kanzari is a cybersecurity expert with an extensive background in IT risk management and cybersecurity instruction. With a diverse range of certifications that includes being a PECB Certified Trainer, DORA Senior Lead Manager, NIST Cybersecurity Consultant, Senior Lead Incident Manager, Senior Lead SOC 2 Analyst, Data Protection Officer (DPO), DORA Senior Lead Manager, ISO 42001 Senior Lead Auditor, ISO 42001 Senior Lead Implementer, Senior Lead SCADA Security Manager, ISO 22301 Senior Lead Implementer, ISO 22301 Senior Lead Auditor,EBIOS Risk Manager, ISO 27005 Senior Lead Risk Manager, ISO 27001 Senior Lead Implementer, ISO 27001 Senior Lead Auditor, Cisco Certified Specialist in Security Core and Enterprise Core, NSE4 Network Security Professional, Palo Alto Instructor, Devops Tools Engineer, LPIC-3 Enterprise Professional Security, LPIC-3 Enterprise Professional Virtualization & High Availability, LPIC-2, LPIC-1, Suse Certified Linux Administration, and a Certified Security Auditor in computer security,

Noureddine Kanzari's professional journey is characterized by a series of impactful roles and accomplishments. Throughout his career, he has held various pivotal positions, including:

Chief Information Security Officer (CISO)

Audit Team Leader

Cybersecurity Instructor

Technical Manager

Training Manager

His extensive experience and leadership have contributed significantly to enhancing cybersecurity practices, risk management strategies, and organizational resilience.

Contents

1. ORGANIZATIONAL CONTROLS

1.1 Acceptable use of information and other associated assets (5.10)

Control 5.10:

Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.

Control attributes:

- Control type: When it acts : Preventive
- Information security properties: Confidentiality, Integrity, Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Protect
- Optional capabilities: Which operational area it belongs to : Asset_management, Information_protection
- Security domains: Which domain it relates to : Governance_and_Ecosystem, Protection

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventive	Confidentiality Integrity Availability	Protect	#Asset_management #Information_protection	#Governance_and_Ecosystem #Protection

Control description:

Everyone who uses company information or systems (staff, contractors, third parties) should know the rules for using and protecting that information.

The company must write a specific policy (set of rules) explaining:

- What is okay to do (expected behavior)
- What is not okay (unacceptable behavior)
- What kind of monitoring the company will do (e.g.tracking internet use)

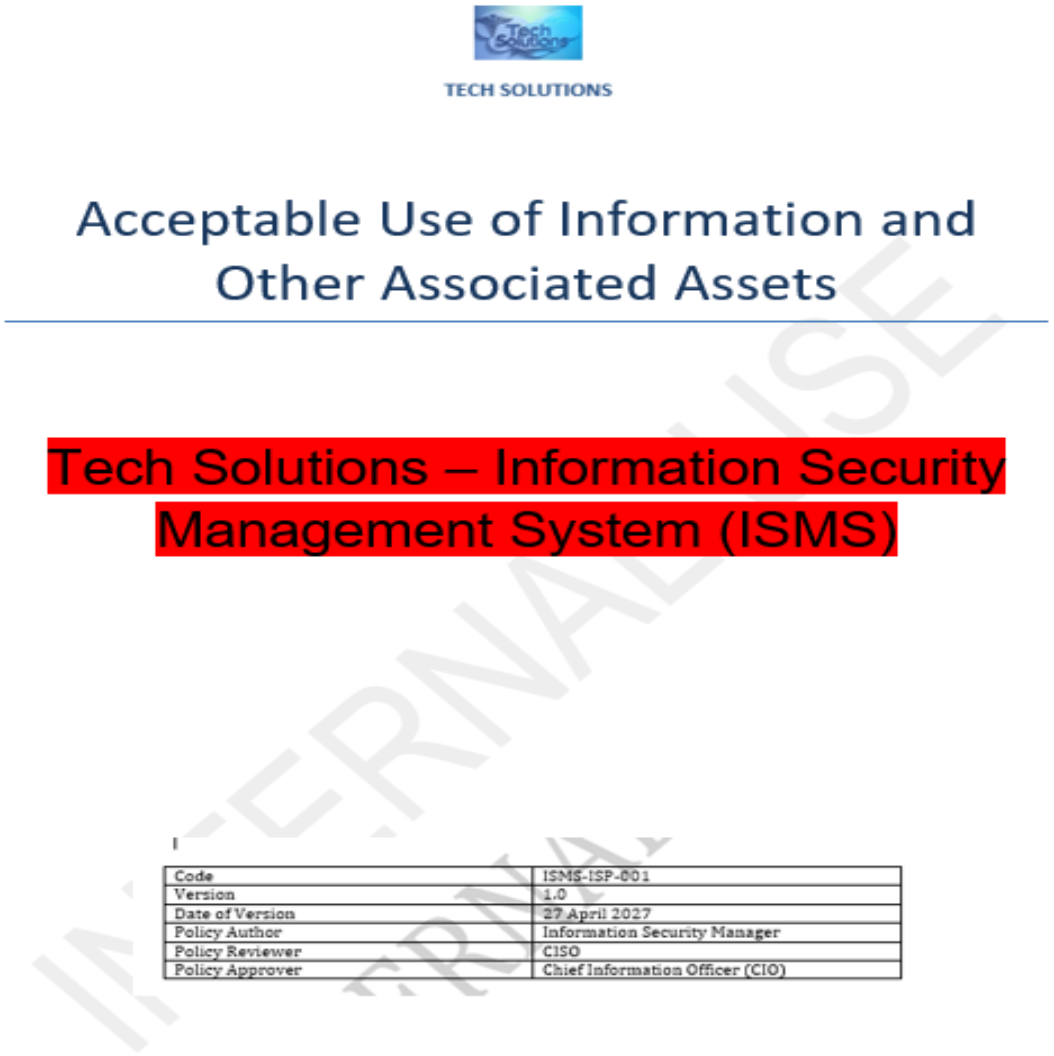
Make sure the rules explain how to use data safely, what is allowed and not allowed, and how data should be protected from start to finish.

Control evidence:

Checks to be performed	Evidence
➢ Whether a specific policy for the proper use of information and other associated assets is developed, implemented, and communicated to anyone who uses or processes information and other associated assets. ➢ Whether staff and external users have been made aware of the security requirements contained in this policy and of their responsibility for the use of any information processing means. ➢ Whether procedures for the proper use of information and associated assets, based on their classification and identified risks, are developed and implemented.	➢ Specific policy for the proper use of information and other associated assets ➢ Procedures for the proper use of information and associated assets

1.2 Practical Application of Clause 5.10: Case Study: ”Tech Solutions”

The Acceptable Use document defines how Tech Solutions' digital assets must be used securely, ensuring compliance with legal and regulatory standards. It protects sensitive data (especially medical and proprietary information) from misuse, breaches, and unauthorized access by establishing clear user responsibilities:



TECH SOLUTIONS

Acceptable Use of Information and Other Associated Assets

Tech Solutions – Information Security Management System (ISMS)

Code	ISMS-ISP-001
Version	1.0
Date of Version	27 April 2027
Policy Author	Information Security Manager
Policy Reviewer	CISO
Policy Approver	Chief Information Officer (CIO)

Change History

Version	Date	Action	Created by
1.0	27 April 2025	Basic Document	Information Security Manager

Contents

18. Monitoring and Audit

System activity (network traffic, emails, access logs) is monitored in compliance with GDPR.

Users are informed of monitoring during onboarding.

Audits are conducted biannually, with third-party penetration tests performed yearly.

19. Incident Reporting

All security incidents (malware, data breach, unauthorized access) must be reported to the ISO within 24 hours.

Report via security@techsolutions.com or hotline +1-800-555-1234.

An incident response plan ensures containment, eradication, and recovery.

20. Violations and Sanctions

Minor infractions: verbal/written warning. Repeated offenses may escalate.

Serious breaches: suspension, access revocation, termination, or legal action.

Employees may appeal sanctions within 7 days to HR and ISO.

21. Review and Updates

Policy is reviewed annually or upon major changes to operations or law.

Updates are reviewed by ISO, legal, and general management, and communicated through email and meetings.

22. Acknowledgment

I, [Name], acknowledge reading and understanding this policy.

I agree to comply and understand that violations may result in disciplinary action.

Name: _____ Employee ID: _____

Department: _____ Date: _____

Signature: _____

12. Intellectual Property Rights (Copyright)

Users must respect copyright and licensing agreements of all software and media.

All internal developments, documents, and intellectual property are the exclusive property of Tech Solutions.

Unauthorized copying, use, or distribution of copyrighted materials is forbidden.

13. Operational Security

Antivirus and endpoint protection must be active and up to date on all devices.

Users are not permitted to disable security tools or system configurations set by IT.

Known vulnerabilities must be patched in accordance with their severity (CVSS ≥7 immediately).

14. Business Continuity

Critical systems are backed up daily (incremental) and weekly (full).

Backups are encrypted, stored securely, and verified weekly.

Recovery procedures are tested every quarter.

15. Remote Work and Mobility

All remote workers must use company-issued, MDM-managed devices.

Remote sessions require VPN access, MFA, and adherence to workstation security practices.

Personal devices may not be used unless explicitly authorized and enrolled in MDM.

16. Social Media and Ethical Conduct

Employees must not disclose confidential information or damage Tech Solutions' reputation online.

Official posts require approval from communications or ISO.

Personal social media must clarify that opinions are individual, not representative of Tech Solutions.

17. Training and Awareness

New employees must complete onboarding security training within the first 30 days.

Annual refresher training and quarterly awareness campaigns are mandatory for all employees.

Simulated phishing exercises are conducted to test awareness, with follow-up training where needed.

Instant messaging tools such as Teams, Slack, or equivalent must follow the same usage rules as email.

Messages must avoid offensive, discriminatory, or defamatory content. Company communication must remain courteous and professional.

7. Use of Printers, Scanners, and Copiers

Only use for business needs; printing personal material is discouraged.

Collect all printouts promptly to avoid data exposure.

Secure or confidential material should use secure print features.

8. Software Installation on User Devices

All software must be requested via a formal software request form and be vetted by the ISO.

Open-source and freeware tools must undergo security assessment prior to use.

Self-installation of software, even for development purposes, requires prior authorization.

9. Use of Removable Media

Removable media (USBs, external drives) must be encrypted and approved by IT before use.

All devices must be scanned with antivirus before connecting to any system.

Users must avoid using personal storage devices for work purposes.

10. Data Protection and Medical Data Security

Data must be classified according to Tech Solutions' data classification policy: Public, Internal, Confidential, or Restricted.

Restricted data such as patient medical records or source code must be encrypted at rest and in transit.

Transfers to third parties must follow strict encryption and logging protocols, with written approval from the ISO.

11. Password Management

Passwords must be complex (minimum 12 characters, including uppercase, lowercase, numbers, and symbols).

They must be changed every 30 days and never reused or shared.

MFA is mandatory for all cloud services and sensitive environments.

1. Introduction

This Acceptable Use Policy (AUP) provides a comprehensive framework for secure, ethical, and legal use of Tech Solutions' IT resources. It supports our obligations under GDPR, HIPAA, ISO 27001, and NIS 2, and reflects our commitment to protecting medical and proprietary data.

2. Scope

This policy applies to all users of Tech Solutions' resources, including employees, contractors, third-party vendors, and clients with authorized system access, whether working on-site or remotely.

3. General Principles

Users must act responsibly, professionally, and in alignment with company values. Any use that could compromise system security or company reputation is prohibited.

This policy supports confidentiality, integrity, and availability of all data and systems.

4. Access and Authentication

Access is granted based on role-specific needs using Role-Based Access Control (RBAC).

Multi-Factor Authentication (MFA) is required for all sensitive or externally accessible systems.

Accounts are monitored for unauthorized access and immediately revoked upon termination.

5. Use of Workstations, Networks, and Software

All company computers and laptops must be encrypted and secured using MDM solutions.

Network access must be conducted over secure, encrypted channels (e.g., VPN, HTTPS).

Only IT-approved software may be installed; unauthorized installations are forbidden.

6. Internet, Email, and Messaging Systems

The internet is to be used for professional activities related to Tech Solutions' operations. Accessing inappropriate, illegal, or harmful content is strictly prohibited.

All internet traffic is subject to monitoring. Bandwidth-intensive personal activities (e.g., streaming, torrenting) are not allowed.

Email must be used professionally. Personal messages should be minimal, with sensitive communications encrypted.

1.3 Return of assets (5.11)

Control 5.11:

Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

Control attributes:

- Control type: When it acts : Preventive
- Information security properties: Confidentiality, Integrity, Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Protect
- Optional capabilities: Which operational area it belongs to : Asset_management
- Security domains: Which domain it relates to : Protection

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventive	Confidentiality Integrity Availability	Protect	Asset_management	Protection

Control description:

Make sure the organization collects back all assets that were given to someone to do their job, especially those that might contain sensitive information or give access to systems.

How:

- Keep a list of all the things an employee or partner was given when they started (like a checklist).
- Before or on their last day, make sure everything on the list is returned.

Why:

- Prevents data leaks or misuse after someone leaves.
- Keeps the organization secure and compliant with laws like GDPR or HIPAA.
- Avoids loss or theft of valuable assets.

Control evidence:

Checks to be performed	Evidence
➢ Whether the return of assets in the possession of personnel and other interested parties at the end of the employment is documented ➢ Whether, during the notice period and thereafter, the organization controls unauthorized copying of relevant information	➢ Checklist prohibiting unauthorized copies of relevant information during and after the notice period ➢ PVS of receipt of assets in possession

1.4 Practical Application of Clause 5.11: Case Study: ”Tech Solutions”

The following Form is a structured document used to ensure that all company-issued information assets such as laptops, mobile devices, access tokens, documents, and sensitive data are properly returned by departing employees, contractors, or third parties:

TECH SOLUTIONS

Tech Solutions

INFORMATION ASSET RETURN CONFIRMATION FORM

Code	ISMS-ISP-001
Version	1.0
Date of Version	27 April 2027
Policy Author	Information Security Manager
Policy Reviewer	CISO
Policy Approver	Chief Information Officer (CIO)

Change History

Version	Date	Action	Created by
1.0	27 April 2025	Basic Document	Information Security Manager

Contents

1. Purpose

This form is used to confirm the return of all information and physical assets provided to an employee, contractor, or third-party user by Tech Solutions. It ensures that no sensitive data or proprietary equipment remains in the possession of the departing individual, thereby protecting the company's information security and regulatory compliance (e.g., GDPR, HIPAA, ISO 27001, NIS 2).

2. Departing Individual Information

Full Name: _____

Job Title / Department: _____

Date of Departure: _____

Manager's Name: _____

3. Information and Associated Assets to Be Returned

The individual must return all of the following (as applicable):

- Laptops, desktops, and tablets (with serial numbers)
- Mobile phones and GSM chips
- External drives, USBs, and SD cards
- Access cards, smartcards, and authentication tokens (e.g., Yubikeys)
- Source code, software licenses, and development environments
- Internal/external documentation (manuals, reports, technical docs)
- Physical files or printouts containing sensitive or proprietary data
- Email and intranet access credentials
- Seals or stamps bearing the Tech Solutions name

4. Asset Return Log

No.	Asset Description (ID/SN)	Condition	Date Returned	Receiver Name & Signature
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

5. Departing Individual Declaration

I declare that I have returned all information assets in my possession provided by Tech Solutions, as outlined above and in the Asset Return Agreement.

Location: _____ Date: _____

Signature: _____

6. Line Manager Confirmation

I confirm that the above-named individual has returned all Tech Solutions assets including physical items, source code repositories, cloud resources, customer documentation, and emails.

Name: _____ Department: _____

Signature: _____ Date: _____

7. Information Security Department Approval

I approve that all listed assets have been returned and validated by the IT Infrastructure or Information Security team.

Name: _____ Department: _____

Signature: _____ Date: _____

1.5 Classification of information (5.12)

Control 5.12:

Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.

Control attributes:

- Control type: When it acts : Preventive
- Information security properties: Confidentiality, Integrity, Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Identify
- Optional capabilities: Which operational area it belongs to : Information_protection
- Security domains: Which domain it relates to : Protection, Defense

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventive	Confidentiality Integrity Availability	Identify	Information_pro- tection	Protection Defense

Control description:

- The organization should have a specific policy that explains how to label and protect information based on its importance.
- Protect information depending on how it's used, some may need to be shared, others kept secret.
- Include all types of assets, NOT just files, devices and systems that handle the information should be protected according to the same classification.
- The person in charge of the information must decide its classification.
- The policy should explain how to classify info and when to review/update it.
- The higher the damage if info is leaked, changed, or lost, the higher its classification level.
- Everyone should use the same system to avoid confusion and ensure proper protection.

Control evidence:

Checks to be performed	Evidence
➢ Whether a specific information classification policy is established and communicated to relevant stakeholders ➢ Whether non-information assets are classified in accordance with the classification of the information they store, process, handle, or protect ➢ Whether class-specific security measures are applied in accordance with the classification system.	➢ Specific policy on the classification of information

1.6 Practical Application of Clause 5.12: Case Study: ”Tech Solutions”

The following Information Classification Policy of Tech Solutions establishes a comprehensive framework for identifying, labeling, and managing information based on its sensitivity, legal obligations, and operational importance. It defines four classification levels: Public, Internal, Confidential, and Restricted, each with specific handling, access control, storage, and disposal requirements:

Information Classification Policy

Code	ISMS-ISP-001
Version	1.0
Date of Version	27 April 2027
Policy Author	Information Security Manager
Policy Reviewer	CISO
Policy Approver	Chief Information Officer (CIO)

Change History

Version	Date	Action	Created by
1.0	27 April 2025	Basic Document	Information Security Manager

Contents

Copyright

1. Introduction

1.1 Purpose

The Information Classification Policy establishes a structured framework for identifying, classifying, handling, and protecting information assets at Tech Solutions. This policy ensures compliance with legal and regulatory requirements (e.g., GDPR, HIPAA, ISO 27001, NIS 2) while safeguarding sensitive medical data, proprietary source code, and other critical assets. The objectives are to:

- Protect the confidentiality, integrity, and availability of information.
- Define clear guidelines for handling data based on its sensitivity and criticality.
- Mitigate risks of data breaches, unauthorized access, or misuse.
- Support secure software development (DevSecOps), cloud hosting, and e-commerce operations.
- Ensure consistent data protection practices across physical offices, remote work environments, and internal/external data centers.

1.2 Scope

This policy applies to:

- **Information**: All data created, stored, processed, or transmitted by Tech Solutions, including medical records, customer data, source code, financial records, and operational documentation, in digital or physical form.
- **Assets**: Systems and resources handling information, including servers (internal and external data centers), workstations, laptops, mobile devices, networks (internal, VPN, cloud), critical applications (Online Medical Platform, customer database, financial systems), and e-commerce website.
- **Users**: All employees (100 across General Management, IT Development, Customer Support, Human Resources, Sales and Marketing, IT Infrastructure, Information Security and Compliance), contractors, vendors, clients accessing systems via extranet, and third parties.
- **Locations**: Two physical offices, internal data centers hosting development servers, and external data centers hosting client cloud services.

1.3 Audience

This policy is mandatory for all users interacting with Tech Solutions' information assets, including:

- Full-time and temporary employees, with 40% working remotely.
- Contractors and vendors involved in software development, cloud hosting, or support services.
- Clients accessing the Online Medical Platform or extranet.
- Third-party service providers with access to networks or data.

All users must acknowledge and sign this policy to confirm compliance.

1.4 Compliance

Non-compliance with this policy violates Tech Solutions' employee code of conduct and may result in disciplinary action, including termination, as well as legal or financial penalties. Exceptions require written approval from the Information Security Officer (ISO). Users must report violations or incidents to the ISO at security@techsolutions.com within 24 hours.

1.5 Contact

For inquiries or incident reporting, contact:

- **Information Security Officer**: security@techsolutions.com, +1-800-555-1234.
- **IT Infrastructure Support**: it.support@techsolutions.com.

---

2. Definitions

- **Information Asset**: Any data or resource (digital or physical) with value to Tech Solutions, including medical data, source code, and financial records.
- **Information Security Officer (ISO)**: The Director of Information Security, responsible for policy enforcement and compliance with GDPR, HIPAA, ISO 27001, and NIS 2.
- **Sensitive Data**: Information requiring protection due to its confidentiality, integrity, or availability, such as personally identifiable information (PII), medical records, or proprietary source code.
- **Critical Applications**: Systems essential to operations, including the Online Medical Platform, customer database, financial systems, and e-commerce website.
- **DevSecOps**: Security-integrated software development practices.
- **Data Owner**: The individual or department responsible for classifying and managing specific data sets.

---

3. Information Classification Levels

Information at Tech Solutions is classified into four levels based on its sensitivity, criticality, and regulatory requirements. Each level defines specific handling, storage, access, and disposal requirements.

3.1 Public

- **Description**: Information intended for public disclosure with no confidentiality requirements.
- **Examples**:

    - Marketing materials (e.g., brochures, website content).
    - Publicly available product descriptions.
    - Press releases and public announcements.
- **Handling Requirements**:
    - No restrictions on access or distribution.
    - May be shared externally without approval.
    - Stored on accessible systems (e.g., e-commerce website, public cloud storage).
- **Security Controls**:
    - Minimal; ensure accuracy and integrity to maintain brand reputation.
    - No encryption required.
- **Regulatory Compliance**: None specific, but must align with advertising and intellectual property laws.

3.2 Internal

- **Description**: Information for internal use only, not sensitive but requiring limited access to prevent misuse.
- **Examples**:
    - Internal policies and procedures (e.g., HR guidelines, IT manuals).
    - Non-sensitive employee communications (e.g., newsletters).
    - General project documentation without confidential data.
- **Handling Requirements**:
    - Accessible to employees and authorized contractors with a business need.
    - Not to be shared externally without manager approval.
    - Stored on internal servers or secure cloud platforms with access controls.
- **Security Controls**:
    - Role-based access control (RBAC) to restrict to authorized users.
    - Basic encryption (e.g., TLS for transmission).
    - Logging of access for audit purposes.
- **Regulatory Compliance**: ISO 27001 for access control and integrity.

3.3 Confidential

- **Description**: Sensitive information requiring strict access controls due to business or regulatory impact if disclosed.
- **Examples**:
    - Customer PII (e.g., names, contact details, non-medical data).
    - Proprietary source code for the Online Medical Platform and other applications.
    - Financial records (e.g., billing data, vendor contracts).
    - Sales and marketing strategies.
- **Handling Requirements**:
    - Access restricted to specific roles (e.g., IT Development for source code, Sales for customer data).
    - External sharing requires ISO approval and encryption.
    - Stored on encrypted servers (internal or external data centers) with RBAC and multi-factor authentication (MFA).
    - Physical copies stored in locked cabinets.
- **Security Controls**:

    - AES-256 encryption for storage and transfer.
    - Mandatory MFA for access.
    - Regular access reviews (quarterly).
    - Audit trails for all access and modifications.
- **Regulatory Compliance**: GDPR (data minimization, consent), ISO 27001 (confidentiality), NIS 2 (critical system protection).

3.4 Restricted

- **Description**: Highly sensitive information with severe legal, financial, or operational consequences if compromised, including health data subject to stringent regulations.
- **Examples**:
    - Medical records in the customer database (e.g., patient diagnoses, treatment plans).
    - Sensitive financial transactions (e.g., payment card data).
    - Critical system credentials (e.g., cloud server admin accounts).
    - Intellectual property under development (e.g., unreleased software algorithms).
- **Handling Requirements**:
    - Access limited to a minimal number of authorized personnel (e.g., specific IT Development or Customer Support staff).
    - External sharing prohibited without ISO and Data Protection Officer (DPO) approval.
    - Stored on dedicated, encrypted servers in secure data centers with physical and logical access controls.
    - Physical copies prohibited unless absolutely necessary, stored in safes, and tracked.
- **Security Controls**:
    - AES-256 encryption at rest and in transit.
    - Mandatory MFA and biometric authentication for critical systems.
    - Real-time monitoring and anomaly detection.
    - End-to-end encryption for all transfers.
    - Data loss prevention (DLP) tools to prevent unauthorized exfiltration.
- **Regulatory Compliance**: GDPR (data subject rights), HIPAA (patient confidentiality), ISO 27001 (high-risk data), NIS 2 (critical infrastructure).

---

4. Roles and Responsibilities

4.1 Information Security Officer (ISO)

- Oversees policy implementation and compliance.
- Approves exceptions, classifications, and external data sharing.
- Conducts incident investigations and audits.

4.2 Data Owners

- Department heads (e.g., IT Development, Customer Support) responsible for specific data sets.
- Classify data according to this policy.
- Define access requirements and review permissions quarterly.
- Ensure proper handling and disposal of their data.

4.3 Employees and Users

- Classify data they create or handle per this policy.
- Follow handling, storage, and access guidelines for each classification level.
- Report misclassified data or incidents to the ISO immediately.
- Complete mandatory training on data classification and security.

4.4 IT Infrastructure Department

- Implements technical controls (e.g., encryption, RBAC, DLP) for classified data.
- Manages secure storage and backup systems.
- Monitors access logs and enforces security configurations.

4.5 Information Security and Compliance Department

- Conducts regular audits and risk assessments.
- Provides training and awareness programs.
- Ensures alignment with GDPR, HIPAA, ISO 27001, and NIS 2.

---

5. Classification Process

5.1 Identifying Information Assets

- Data owners must inventory all information assets within their department (e.g., databases, source code repositories, financial records).
- Assets are evaluated for sensitivity, criticality, and regulatory requirements.

5.2 Assigning Classification Levels

- Data owners classify assets as Public, Internal, Confidential, or Restricted based on Section 3 criteria.
- Classification considers:
  - Legal obligations (e.g., GDPR for PII, HIPAA for medical data).
  - Business impact (e.g., loss of source code confidentiality).
  - Operational criticality (e.g., cloud service availability).
- Ambiguous cases are escalated to the ISO for final determination.

5.3 Labeling

- **Digital Data**:
  - Metadata tags (e.g., "Restricted: Medical Data") applied to files and databases.
  - Email headers include classification labels (e.g., "[Confidential]" in subject line).
- **Physical Data**:
  - Documents stamped with classification level (e.g., "Restricted" watermark).
  - Stored in color-coded folders (e.g., red for Restricted, blue for Confidential).
- Automated tools (e.g., DLP software) enforce labeling for sensitive data.

5.4 Review and Reclassification

- Classifications are reviewed annually or upon significant changes (e.g., new regulations, data usage shifts).
- Data owners submit reclassification requests to the ISO if sensitivity changes (e.g., public release of previously Confidential data).

---

6. Handling and Storage Requirements

6.1 Storage

- **Public**: Stored on accessible systems (e.g., e-commerce website, public cloud).
- **Internal**: Stored on internal servers or secure cloud platforms with RBAC.
- **Confidential**: Stored on encrypted servers (AES-256) with MFA and audit logging.
- **Restricted**: Stored on dedicated, encrypted servers in secure data centers with physical access controls and biometric authentication.
- Local storage on workstations or mobile devices is prohibited for Confidential and Restricted data unless encrypted and synchronized to secure servers.

6.2 Transmission

- **Public**: No encryption required; use standard protocols (e.g., HTTP).
- **Internal**: Use secure protocols (e.g., HTTPS, TLS).
- **Confidential**: Use AES-256 encryption and secure channels (e.g., SFTP, VPN).
- **Restricted**: Use end-to-end encryption, with passwords sent via separate channels (e.g., phone).
- External transmission of Confidential or Restricted data requires ISO approval and DLP monitoring.

6.3 Access Controls

- **Public**: No access restrictions.
- **Internal**: RBAC based on job function.
- **Confidential**: RBAC, MFA, and quarterly access reviews.
- **Restricted**: RBAC, MFA, biometric authentication, and real-time monitoring.
- Access logs are retained for 12 months for audit purposes.

6.4 Backup and Recovery

- All data is backed up with daily incremental and weekly full backups.
- Backups are encrypted (AES-256) and stored in secure data centers.
- Restricted data backups are isolated to prevent unauthorized access.
- Recovery tests are conducted quarterly to ensure data integrity.

---

7. Disposal and Destruction

7.1 Digital Data

- **Public and Internal**: Deleted using standard file deletion, with no special requirements.
- **Confidential**: Securely wiped using software meeting NIST 800-88 standards (e.g., 3-pass overwrite).
- **Restricted**: Securely wiped with 7-pass overwrite and verified by IT Infrastructure.
- Deleted data is logged for audit purposes.

7.2 Physical Data

- **Public and Internal**: Recycled unless containing sensitive annotations.
- **Confidential**: Shredded using cross-cut shredders (DIN 66399 P-4 standard).
- **Restricted**: Shredded and incinerated, with destruction certified by a third-party vendor.
- Physical disposal is logged and witnessed by two authorized personnel.

---

8. Remote Work and Mobile Devices

- Remote workers (40% of workforce) must use company-issued devices enrolled in the mobile device management (MDM) system.
- Confidential and Restricted data access requires VPN and MFA.
- Local storage on mobile devices is prohibited; data must be accessed via secure cloud applications.
- Devices must have full-disk encryption (e.g., BitLocker) and remote wipe capabilities.
- Lost or stolen devices must be reported to the ISO within 1 hour for remote wiping.

---

9. Training and Awareness

- All users complete mandatory annual training on information classification, covering:
  - Classification levels and handling requirements.

    - GDPR, HIPAA, ISO 27001, and NIS 2 obligations.
    - Incident reporting and secure disposal.
- New hires receive training within 30 days of onboarding.
- Quarterly awareness campaigns (e.g., posters, phishing simulations) reinforce classification practices.
- The intranet hosts guides and FAQs at security.techsolutions.com.

---

10. Monitoring and Auditing

- **Monitoring**:
    - DLP tools monitor data access and transfers for Confidential and Restricted data.
    - Network traffic and access logs are analyzed for anomalies.
    - Monitoring complies with GDPR privacy requirements.
- **Auditing**:
    - Biannual internal audits verify classification compliance.
    - Annual external audits (e.g., ISO 27001 certification) assess policy effectiveness.
    - Audit findings are addressed within 30 days, with reports to the ISO.
- **Incident Reporting**:
    - Misclassification or mishandling incidents must be reported to the ISO within 24 hours.
    - The incident response process (per the Information Security Policy) ensures containment and remediation.

---

11. Non-Compliance

- Violations (e.g., misclassifying data, unauthorized sharing) result in disciplinary action:
    - **Minor**: Verbal/written warning.
    - **Moderate**: Access suspension, mandatory retraining.
    - **Severe**: Termination, legal action.
- Users are liable for damages caused by non-compliance (e.g., regulatory fines, data breaches).
- Exceptions require ISO approval, documented in the security log.

---

12. Policy Review and Updates

- The policy is reviewed annually or after significant changes (e.g., new regulations, system upgrades).

- The ISO and Information Security Committee propose updates, reviewed by General Management and legal counsel.
- Changes are communicated via email, intranet, and team meetings, with user acknowledgment required.

---

13. Annexes

13.1 Glossary

- **AES-256**: Advanced Encryption Standard with 256-bit key for secure data protection.
- **DLP**: Data Loss Prevention, tools to prevent unauthorized data exfiltration.
- **MFA**: Multi-Factor Authentication, requiring multiple verification methods.
- **NIST 800-88**: US standard for secure data sanitization.
- **PII**: Personally Identifiable Information, data that can identify an individual.

13.2 Contacts

- **Information Security Officer**: security@techsolutions.com, +1-800-555-1234.
- **Data Protection Officer**: dpo@techsolutions.com.
- **IT Infrastructure Support**: it.support@techsolutions.com.
- **Intranet**: security.techsolutions.com for resources.

13.3 Declaration of Conformity

I, [Name], acknowledge that I have read, understood, and agree to comply with the Information Classification Policy. I understand my responsibilities for classifying and handling information and commit to reporting incidents promptly.

Name	Employee ID	Department	Date	Signature
.....	.....	.....	.....	.....

1.7 Labelling of information (5.13)

Control 5.13:

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

Control attributes:

- Control type: When it acts : Preventive
- Information security properties: Confidentiality, Integrity, Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Protection
- Optional capabilities: Which operational area it belongs to : Information_protection
- Security domains: Which domain it relates to : Protection, Defense

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventive	Confidentiality Integrity Availability	Protection	Information_pro- tection	Protection Defense

Control description:

- Label all types of information and assets. This includes emails, documents, databases, printed papers, USB drives, cloud files, etc.
- Every kind of storage or format (digital, paper, etc.) should be considered
- The labels should match your organization's classification levels (e.g., Public, Internal, Confidential, and Restricted).
- Make sure labels are clear and visible, like putting “[Confidential]” in a document header
- You may decide not to label information that isn’t sensitive, like marketing brochures or public FAQs, this avoids unnecessary work.
- Labeling across different formats

Example of how to label:

- Emails: Add “[Confidential]” in the subject line.
- Documents: Add headers/footers with classification.
- USB sticks or hard drives: Put physical stickers or tag files inside.
- Cloud or shared folders: Use metadata or folder names.

Control evidence:

Checks to be performed	Evidence
➢ Whether procedures for marking information in accordance with the established classification scheme are developed and implemented.	➢ Information marking procedures

1.8 Practical Application of Clause 5.13: Case Study: ”Tech Solutions”

The Information Marking Procedure at Tech Solutions ensures that all information assets, digital or physical are clearly labeled according to their classification level (Public, Internal, Confidential, or Restricted) to support proper handling, access control, and compliance with regulatory standards:

Information Marking Procedure

Code	ISMS-ISP-001
Version	1.0
Date of Version	27 April 2027
Policy Author	Information Security Manager
Policy Reviewer	CISO
Policy Approver	Chief Information Officer (CIO)

Change History

Version	Date	Action	Created by
1.0	27 April 2026	Basic Document	Information Security Manager

Contents

1. Purpose

This procedure defines how to mark information assets (digital and physical) according to their classification level (Public, Internal, Confidential, Restricted) to ensure proper handling, access control, and compliance with regulatory and security requirements (e.g., GDPR, HIPAA, ISO 27001, NIS 2).

2. Scope

This applies to all employees, contractors, and third-party users handling Tech Solutions' information, across all locations, systems, and devices (e.g., workstations, cloud platforms, mobile devices).

3. Responsibilities

- Data Owners: Ensure correct marking of the information they manage.
- All Users: Apply and respect information markings.
- IT Department: Provide tools for automated tagging and enforce technical controls.
- ISO (Information Security Officer): Oversee compliance and approve exceptions.

4. Marking Principles

- Markings must reflect the classification level defined in the Information Classification Policy.
- Markings should be clear, consistent, and placed in a visible location.
- All digital and physical formats must be included (emails, documents, databases, printouts, etc.).

5. Marking by Classification Level

Classification	Digital Marking Example	Physical Marking Example	Color Code
Public	No label or "[Public]" in footer	None required	Green
Internal	"[Internal]" in header/footer	Printed with "Internal" watermark	Blue
Confidential	"[Confidential]" in subject line, header	Folder with red label, "Confidential" watermark	Red
Restricted	"[Restricted: Medical Data]" in header	Locked file cabinet, label: "Restricted – ISO"	Dark Red

6. Marking Methods

- a. Emails

Add classification in subject line: Example: [Confidential] Q2 Financial Report
Ensure body or attachments reflect classification.
Use automatic classification tools where available (e.g., Outlook Sensitivity Labels).

- b. Documents (Word, PDF, etc.)

Add label in header and/or footer.
Watermarks are recommended for Confidential and Restricted data.
Use document templates pre-configured with classification labels.

- c. Spreadsheets and Presentations

Insert classification in: First slide/page, Header/footer.
Color-code tabs (Excel) where possible.

- d. Databases and Cloud Systems

Use metadata tags to classify datasets or records.
Include classification in record descriptions where applicable.

- e. Removable Media (USBs, DVDs)

Attach physical sticker indicating classification.
Store in locked containers if marked Confidential or Restricted.

- f. Printed Materials

Include a printed label on the top and bottom of the page.
Use color-coded folders: Blue for Internal, Red for Confidential, Dark Red for Restricted.
Store marked physical documents according to their classification.

7. Exceptions

- Omission Cases: Public and clearly non-sensitive materials may be exempt from marking.
- Approval for Changes: All exceptions must be approved in writing by the Information Security Officer (ISO).

8. Enforcement and Auditing

Random audits may verify proper marking compliance.
Improper or missing markings will be reported to the ISO.
Violations may result in disciplinary action.

9. Training and Awareness

New employees are trained within 30 days on marking procedures.
Annual refresher training is mandatory for all users.
Guides and examples are available on the intranet: security.techsolutions.com

1.9 Information transfer (5.14)

Control 5.14:

Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.

Control attributes:

- Control type: When it acts : Preventive
- Information security properties: Confidentiality, Integrity, Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Protection
- Optional capabilities: Which operational area it belongs to : Information_protection, Asset_management
- Security domains: Which domain it relates to : Protection

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventive	Confidentiality Integrity Availability	Protection	Information_pro- Tection Asset_management	Protection

Control description:

- The organization should create a clear policy that explains how information is transferred safely whether by email, USB, spoken conversation, or another method and make sure everyone involved knows and follows the rules.
- Create a Policy for Information Transfer: Make a specific rule about how information should be transferred.
- Share this policy with anyone who needs to know: employees, partners, third parties, etc.
- Information that is more sensitive (e.g. personal or financial data) needs stronger protection during transfer.
- Use proper security measures based on how important or confidential the data is.
- If you send data to another company or external party, make formal agreements (contracts) that say how the data will be protected.

- Make sure the recipient is who they say they are (authentication).
- Apply These Rules to All Transfer Types:
    - Electronic (e.g. email, file sharing)
    - Physical (e.g. USB, printed documents)
    - Verbal (e.g. phone calls, in-person discussions)
- Use tools like encryption (scrambling data so only authorized people can read it).
- Make sure no one can deny sending or receiving the data (non-repudiation).
- List people responsible for the data transfer (like the data owner or IT security officer).
- Clearly mark sensitive or important information with labels (like “Confidential”), so people know how to handle it.
- Make sure the systems used to transfer data (like servers or messengers) work well and are available when needed.
- Define what is acceptable or not when using tools for transferring data (like email or cloud services).

Control evidence:

Checks to be performed	Evidence
➢ Whether a specific policy on the transfer of information is established, implemented and communicated to all interested parties ➢ If this policy covers all types of information transfer: electronic transfer, transfer on physical storage media and verbal transfer ➢ Whether transfer agreements are defined and maintained when information is transferred between the organization and third parties	➢ Specific policy on the transfer of information ➢ Agreements and procedures related to the transfer of information

1.10 Practical Application of Clause 5.14: Case Study: ”Tech Solutions”

Information Transfer Policy

Code	ISMS-ISP-001
Version	1.0
Date of Version	27 April 2027
Policy Author	Information Security Manager
Policy Reviewer	CISO
Policy Approver	Chief Information Officer (CIO)

Change History

Version	Date	Action	Created by
1.0	27 April 2025	Basic Document	Information Security Manager

Contents

1. Purpose

The purpose of this Information Transfer Policy is to ensure the secure and responsible transfer of information within Tech Solution and between Tech Solution and external parties. This policy aims to protect sensitive, confidential, and critical business information against unauthorized access, loss, or compromise during transfer.

2. Scope

This policy applies to all employees, contractors, consultants, and third parties who access, transfer, or receive Tech Solution's information in any form—electronic, physical, or verbal.

3. Policy Statement

Tech Solution is committed to maintaining the confidentiality, integrity, and availability of its information during transfer. All transfers must align with information classification levels and legal, contractual, and regulatory obligations.

4. Classification-Based Transfer Protection

All information must be classified according to Tech Solution's Information Classification Policy. Transfer methods and security controls must reflect the classification:

- **Public**: No special controls.
- **Internal Use Only**: Require basic access controls.
- **Confidential**: Require encryption and access restrictions.
- **Restricted**: Require end-to-end encryption, strict authentication, and audit trails.

5. Methods of Transfer

- **Electronic**: Email, FTP, cloud services, internal systems
- **Physical Media**: USB drives, CDs/DVDs, printed documents
- **Verbal**: Phone, video conferencing, in-person discussions

6. Controls for Secure Transfer

a. Protection from Unauthorized Access

- Use encryption (AES-256, TLS 1.2+) for all confidential and restricted transfers
- Access to transfer tools must require user authentication
- Avoid use of public Wi-Fi; use VPN when remote

b. Traceability and Non-Repudiation

- Maintain logs of all information transfers
- Ensure a chain of custody is documented for physical transfers
- Use digital signatures where applicable

c. Identification of Responsible Contacts

Each transfer must Identify:

- Information Owner
- Risk Owner (if applicable)
- Information Custodian
- Security Officer

d. Incident Responsibility

In case of a data breach or loss:

- Immediately report to the Information Security Team
- Follow Tech Solution's Incident Response Plan
- Document incident, mitigation steps, and responsible party

e. Labelling Requirements

- Use standardized labels: "Public," "Internal," "Confidential," "Restricted"
- Ensure physical and digital media are labeled clearly
- Train staff to recognize and handle labels appropriately

f. Transfer Reliability

- Use reputable and tested services for transfers
- Monitor service uptime and performance
- Maintain backup transfer methods

g. Acceptable Use Guidelines

- Only approved transfer methods should be used
- Personal email, unapproved cloud storage, and messaging apps are prohibited
- Use organization-approved platforms (e.g., Microsoft 365, Secure File Gateway)

h. Retention and Disposal

- Retain transferred information according to Tech Solution's Data Retention Policy
- Use secure deletion tools for digital data
- Shred physical media before disposal

i. Legal and Regulatory Compliance

- Follow data protection laws (e.g., GDPR, CCPA) and industry standards
- Comply with contractual obligations for third-party data
- Ensure any electronic signature usage aligns with local e-signature laws

7. Transfer Agreements with Third Parties

All third-party information transfers must be governed by a formal Information Transfer Agreement (ITA), covering:

- Authentication and access control
- Encryption standards
- Responsibilities in case of breach
- Compliance with this policy and applicable laws

8. Training and Awareness

All relevant staff will receive training on:

- Information classification
- Secure transfer procedures
- Tools and platforms used for data transfer
- Reporting incidents

9. Review and Updates

This policy will be reviewed annually or after any major incident or regulatory change. Updates will be approved by the Information Security Committee.

10. Enforcement Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

1.11 Access control (5.15)

Control 5.15:

Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.

Control attributes:

- Control type: When it acts : Preventive
- Information security properties: Confidentiality, Integrity, Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Protection
- Optional capabilities: Which operational area it belongs to : Identity_and_access_management
- Security domains: Which domain it relates to : Protection

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventive	Confidentiality Integrity Availability	Protection	Identity_and_ac- cess_management	Protection

Control description:

- Identify who needs access to what information or system, and what type of access (e.g. read, write, admin).
- Write a clear policy that explains how access is granted, managed, and removed and share it with all relevant people.
- Ensure that systems and apps are built with access controls.
- Use locks, badges, or biometric systems to control access to physical areas where sensitive systems are located.
- Only give access to people who truly need it based on their job, especially for sensitive or classified information.
- Restrict and carefully monitor high-level access (like admin or superuser accounts).
- Make sure one person doesn't control every step of a sensitive process (e.g. requesting and approving access).
- Access should be granted only after official approval.

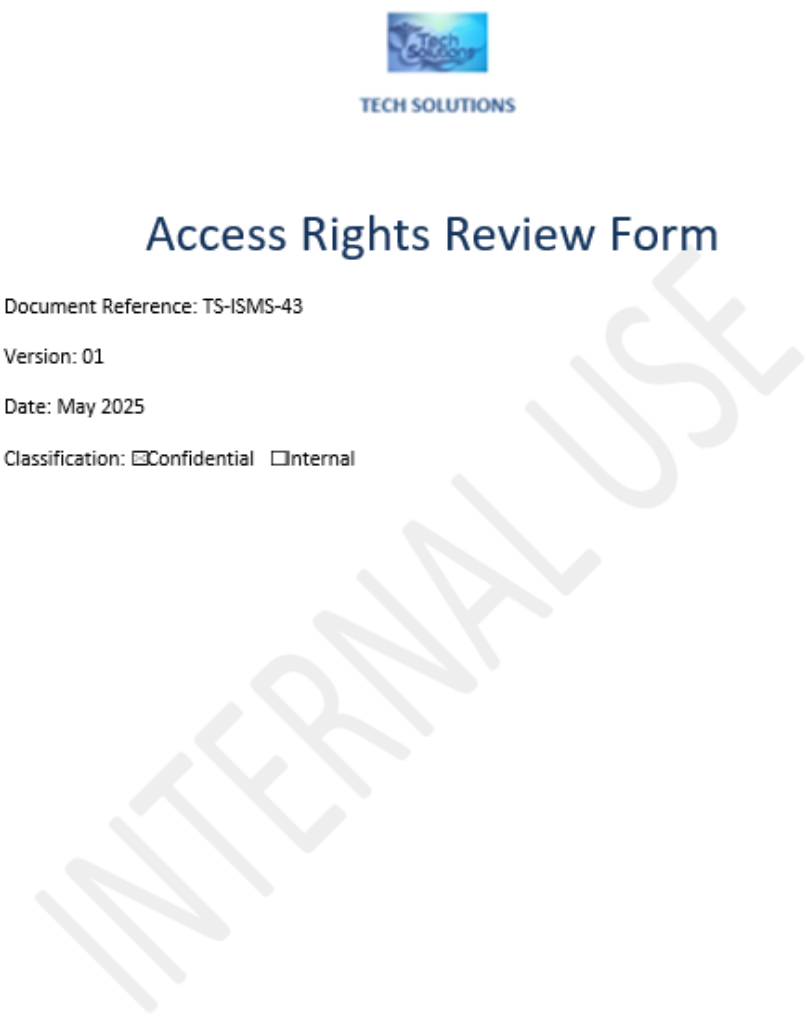
- Regularly review and update who has access, especially when people change jobs or leave the company.
- Keep records of who accessed what and when, to detect misuse or investigate incidents.

Control evidence:

Checks to be performed	Evidence
➢ If business and information security requirements for access control are determined by the owners ➢ Whether the entities that require a defined type of access to information and other associated assets are well determined ➢ Whether an access control policy is developed and implemented ➢ Whether the access rights are consistent with the classification of the information ➢ If access control functions (e.g. access request, access authorization and access administration) are separated ➢ Whether approvals are defined and reviewed regularly	➢ Inventory of information, its owners, the entities that need access to this information ➢ Access control policy ➢ Access control procedures

1.12 Practical Application of Clause 5.15: Case Study: ”Tech Solutions”

The Access Rights Review Form for Tech Solutions is a structured document designed to systematically assess and validate user access to systems and applications within the organization. It captures essential reviewer information, details of the user's access rights including access type, profiles, and business justification and provides sections for reviewer observations and formal approvals by both the Business Owner and Information Security Officer (ISO):



TECH SOLUTIONS

Access Rights Review Form

Document Reference: TS-ISMS-43

Version: 01

Date: May 2025

Classification: ☒Confidential ☐Internal

1. Reviewer Information

Full Name: _____

Phone: _____

Business Unit: _____

Job Title: _____

Review Date (DD/MM/YYYY): _____

Signature: _____

2. Access Review Details

System / Application Name: _____

Module(s): _____

Type of Access Granted (check all that apply):

☐Read ☐Write ☐Modify ☐Delete ☐Admin ☐Execute ☐Other: _____

Access Profile / Group Membership(s): _____

Justification for Access (describe business need):

_____

_____

Last Access Activity Date (if applicable): _____

Account Status: ☐Active ☐Inactive ☐To Be Disabled

3. Reviewer Comments

Provide any observations or recommendations based on access appropriateness, excess rights, or risks.

_____

_____

4. Approval by Business Owner

Name: _____

Title: _____

Date: _____

Signature: _____

Comments:

_____

_____

5. Approval by Information Security Officer (ISO)

Name: _____

Date: _____

Signature: _____

Comments:

_____

_____

6. Additional Notes

Any other remarks, exceptions, or action items identified during the review process.

_____

_____

TECH SOLUTIONS

Access Control Policy

Tech Solutions – Information Security Management System (ISMS)

Code	ISMS-ISP-001
Version	1.0
Date of Version	27 April 2027
Policy Author	Information Security Manager
Policy Reviewer	CISO
Policy Approver	Chief Information Officer (CIO)

Change History

Version	Date	Action	Created by
1.0	27 April 2025	Basic Document	Information Security Manager

Contents

1. OBJECT

Define rules and principles for granting, managing and revoking access to Tech Solutions' information systems, applications and data, to ensure confidentiality, integrity, and availability.

---

2. SCOPE

Applies to all employees, contractors, vendors, third-party users and system/service accounts accessing any Tech Solutions information asset (digital or physical), including networks, servers, applications, databases and devices.

---

3. PURPOSE

Ensure that only appropriately authorized entities obtain the minimum access necessary (least-privilege) to perform their duties (need-to-know / need-to-use), and that all access is traceable, reviewed and compliant with legal, contractual and regulatory obligations.

---

4. PRINCIPLES AND RULES

1. **Least-Privilege & Explicit Permit**
    - Default deny: no access unless explicitly granted.
    - Need-to-know & need-to-use: users only see resources required for their role.
2. **Entity-Access Mapping**
    - Maintain an Access Matrix: list each user/group vs. each asset, with permitted operations.
    - Review and update on role changes or asset additions (ISO 8.26, 5.3, 5.18).
3. **Application Security**
    - Enforce RBAC in all apps; implement session timeouts and parameterized authorization checks.
    - Test access controls during development (authorization fuzzing) and before production release.
4. **Physical-Logical Consistency**
    - Link badge-access revocation to automatic disablement of all logical accounts.
    - Align physical entry controls (badges, biometrics) with logical access rights (ISO 7.2 – 7.4).
5. **Classification Alignment**
    - Apply controls per classification label (Public, Internal, Confidential, Restricted).
    - E.g. Restricted data requires MFA, encryption in transit and quarterly access review (ISO 5.10, 5.12, 5.13).
6. **Privileged Access Restrictions**

    - Separate admin accounts from regular user accounts; no dual-use.
    - Record all privileged sessions and review weekly (ISO 8.2).
7. **Segregation of Duties**
    - Separate roles for request, approval and provisioning of access.
    - No individual may self-approve or both request and implement their own access (ISO 5.3).
8. **Legal & Contractual Compliance**
    - Enforce GDPR/HIPAA/etc. obligations: only users with documented legal basis may access regulated data.
    - Include access-control clauses in third-party contracts
    - Define distinct workflows for:
        - Access Request (Form 1)
        - Access Approval (Manager + ISO)
        - Access Implementation (IT)
    - Log each step for auditability.
9. **Formal Authorization**
    - No access without signed approvals from both Business Owner and
10. **Dynamic Access Controls**
    - Automatically adjust or revoke access when data classification changes or risk factors arise.
11. **Connection-Type Filtering**
    - Only permit connections (VPN, corporate LAN) authorized per role; block all others.
12. **Adaptive Authentication**
    - Increase authentication strength (additional factors) for high-risk logins (new location, off-hours).
13. **Logging & Monitoring**
    - Log all successful and failed access attempts centrally.
    - Generate real-time alerts on anomalies (e.g. off-hours admin actions

---

5. DETAILED DESCRIPTION OF IDENTIFICATION

- **Unique IDs**: every user/system/service must have a unique identifier.
- **Naming Conventions**: differentiate internal, external, privileged and service accounts.
- **Account Creation/Modification**: handled centrally; only upon formal request.
- **Shared Accounts**: prohibited except with formal justification, tracked via a single responsible owner.
- **Connection Filtering**: network access limited by role via firewall/VPN policies.

---

6. DETAILED DESCRIPTION OF AUTHENTICATION

- **Password Rules** (see Annex 1): min. 12 chars, mix of uppercase/lowercase/digits/symbols, rotate every 90 days.
- **MFA**: required for admin, remote, and Restricted-data access.
- **Adaptive Controls**: step-up authentication if risk conditions detected.
- **Lockout**: 5 failed attempts → 15 min lock. Exponential back-off or admin unlock.

- **Session Controls**: inactivity timeout after 15 min (shorter for privileged).
- **PIN & Token Confidentiality**: same protections as passwords.
- **Re-authentication**: required on privilege elevation or after inactivity.

---

7. DETAILED DESCRIPTION OF ACCESS RIGHTS MANAGEMENT

- **Formal Requests**: all rights via Form 1; include business justification.
- **Approvals**: direct manager + ISO sign-off mandatory.
- **Role-Based Profiles**: pre-defined per job function.
- **Lifecycle**: auto-review on role change; revoke within 24 hrs of termination.
- **Orphaned Rights**: expire after 7 days if no owner assigned.

---

8. DETAILED DESCRIPTION OF LOGGING

- **Comprehensive Logs**: record user ID, timestamp, asset, action, source IP.
- **Retention**: store logs ≥ 12 months.
- **Non-Repudiation**: digitally sign critical log entries.
- **Protection**: logs cannot contain actual credentials or hashes.
- **Review**: monthly security-team audit; alerts for anomalies.

---

9. ACCOUNT & ACCESS RIGHTS REVIEWS

- **Annual Reviews**: Data Owners + ISO review all accounts → certify or revoke.
- **Privileged Accounts**: reviewed quarterly.
- **Stale/Orphaned Accounts**: flagged monthly; disabled after 30 days.
- **KPI Monitoring**:
  - Time-to-revoke ≤ 24 hrs
  - Stale-account rate < 1%

---

10. DOCUMENT REVISION

- Reviewed annually or upon major system/regulation changes.
- Revision history logged; approvals by InfoSec Committee.

---

11. NON-CONFORMITY

- Violations treated as security incidents.
- Possible sanctions: warnings, access suspension, termination.
- All incidents logged; corrective actions tracked to closure.

---

12. RESPONSIBILITIES

- **Users**: follow policy; report anomalies.
- **Managers**: validate requests; ensure proper role assignments.
- **IT**: enforce technical controls; process requests.
- **ISO**: maintain policy; audit compliance; manage exceptions.

---

13. DOCUMENT OWNER

Information Security Officer (ISO)
Email: security@techsolutions.com | Tel: +1-800-555-1234

---

14. REFERENCE DOCUMENTS

- ISO/IEC 27001 & 27002
- Tech Solutions Information Classification Policy
- Tech Solutions Asset Management Policy
- NIST SP 800-53

ANNEX 1: PASSWORD POLICY FOR SERVERS & SENSITIVE SYSTEMS

Parameter	Value
Minimum length	16 characters
Complexity	3 of 4 types: upper/lower/digit/special
Rotation interval	Every 90 days
Lockout threshold	5 invalid attempts
Lockout duration	15 minutes
Default-account reset	Admin reset only, no view of old password
History	Prevent reuse of last 5 passwords