ISO/IEC 27002:2022

Mastering the Essentials of Information Security Controls

Your Practical Path to ISO/IEC 27001 Certification

Avoid Minor and Major Non-Conformities

Learn by Doing: Practical Guide

Noureddine Kanzari

Part 4

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 (5.16)

Control 5.16:

The full life cycle of identities should be managed.

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 : 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	Protect	Identity_and_ac- cess_management	Protection

Control description:

- Identity management, which is about controlling and securing the identities (like user accounts)
- Each person should have their own unique identity (like a username or account) in the system, so that any actions they take (e.g., accessing files, making changes) can be traced back to them. This ensures accountability.
- Sometimes, multiple people might share one identity (e.g., a generic “Admin” account). This is only allowed if there’s a valid business or operational reason (e.g., a team needs a shared account for a specific task). These shared accounts need special approval and must be documented properly.
- Identities assigned to non-human entities (like software, bots, or devices) must be managed carefully. These identities need separate approval processes and ongoing monitoring
- If an identity is no longer needed (e.g., an employee leaves the company, changes roles, or a device is decommissioned), it should be disabled or deleted promptly.

- If an identity is no longer needed (e.g., an employee leaves the company, changes roles, or a device is decommissioned), it should be disabled or deleted promptly.
- Within a specific system or domain, one entity (person, device, etc.) should only have one identity.
- The organization must keep logs of important events related to identities, such as:
    - Creating or deleting accounts.
    - Changing permissions.

  These records help track who did what and when, which is useful for audits or investigating security incidents.

➔ The goal is to: Make sure every action can be linked to a specific person or entity.

Control evidence:

Checks to be performed	Evidence
➢ If an identity management process is defined, documented and implemented ➢ Whether the identities assigned to people are unique ➢ If the use of shared identifiers is only allowed when necessary ➢ If unused identities are deactivated or deleted ➢ Whether events related to identity management and authentication information are retained ➢ If an access management procedure is defined and implemented ➢ Whether redundant user IDs are periodically identified and removed or disabled.	➢ Access management procedure.

1.2 Practical Application of Clause 5.16: Case Study: ”Tech Solutions”

TECH SOLUTIONS

Tech Solutions Access Control 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

This Access Control Policy establishes guidelines for managing identities and access to Tech Solutions' information systems, networks, applications, and data. It ensures compliance with ISO 27002 identity management requirements, GDPR, HIPAA, ISO 27001, and NIS 2, while protecting sensitive medical data, source code, and client-facing services.

2. Scope

This policy applies to:

- All employees, contractors, and third parties accessing Tech Solutions' systems.
- All identities (human and non-human) used in internal networks, cloud servers, critical applications (e.g., Online Medical Platform), customer databases, financial systems, and e-commerce websites.
- Physical and remote access to company premises, internal data centers, and systems.

3. Definitions

- **Identity**: A unique identifier (e.g., username, account) assigned to a person, device, or application.
- **Entity**: A person, device, or software process associated with an identity.
- **Authentication**: The process of verifying an identity (e.g., via passwords, multi-factor authentication [MFA]).
- **Authorization**: The process of granting permissions to an identity based on their role.

4. Policy Statements

4.1 Unique Identities for Individuals

- **Requirement**: Each person (employee, contractor, or third party) must have a unique identity linked to them alone to ensure accountability for actions performed.
- **Implementation**:
  - Each employee is assigned a unique user account (e.g., jdoe@techsolutions.com) tied to their employee ID.
  - Accounts are created in the Identity and Access Management (IAM) system (e.g., Active Directory or Okta) during onboarding by the Human Resources (HR) and Information Security teams.
  - Actions performed using an identity (e.g., accessing the customer database or modifying source code) are logged and traceable to the individual.
  - Example: Developers in the IT Development department use unique accounts to access code repositories, ensuring all code changes are attributable.

4.2 Shared Identities

- **Requirement**: Shared identities (used by multiple persons) are only permitted for necessary business or operational reasons, with dedicated approval and documentation.

- **Implementation**:
  - Shared identities are restricted to specific use cases, such as temporary access to a testing environment or a shared customer support account for the Customer Support team.
  - Requests for shared identities must be submitted to the Information Security team, approved by the department head, and documented in the IAM system with:
    - Purpose of the shared identity.
    - List of authorized users.
    - Duration of use (e.g., project-based or permanent).
  - Shared accounts require MFA and are monitored for unusual activity.
  - Example: A shared "SupportTeam" account for the Customer Support department to access the ticketing system is approved for operational efficiency, with documented users and quarterly reviews.

4.3 Non-Human Identities

- **Requirement**: Identities assigned to non-human entities (e.g., servers, applications, or bots) are subject to segregated approval and independent ongoing oversight.
- **Implementation**:
  - Non-human identities (e.g., service accounts for cloud servers or API keys for the Online Medical Platform) are created only after approval by the Information Security team and the IT Infrastructure team.
  - These identities are stored in a secure vault (e.g., HashiCorp Vault) and rotated regularly (every 90 days).
  - Non-human identities are monitored by a Security Information and Event Management (SIEM) system to detect unauthorized use.
  - Example: A service account for the cloud hosting service is approved separately from human accounts and monitored for unusual access patterns.

4.4 Timely Disabling or Removal of Identities

- **Requirement**: Identities no longer required (e.g., due to employee departure, role change, or decommissioned devices) must be disabled or removed promptly.
- **Implementation**:
  - HR notifies the Information Security team within 24 hours of an employee's departure or role change.
  - The Information Security team disables accounts within 48 hours of notification and deletes them after 30 days unless required for audit purposes.
  - Role changes trigger an immediate review of access permissions to align with the new role (e.g., a developer moving to Sales loses access to code repositories).
  - Decommissioned devices or applications have their associated identities disabled within 48 hours by the IT Infrastructure team.
  - Example: When a developer leaves Tech Solutions, their account is disabled, and access to the internal data center and code repositories is revoked within 48 hours.

4.5 No Duplicate Identities

- **Requirement**: A single identity is mapped to a single entity within a specific domain, avoiding duplicate identities.
- **Implementation**:
  - The IAM system enforces unique identifiers (e.g., email-based usernames) to prevent duplicate accounts for the same person or device in the same system.
  - During account creation, the Information Security team verifies that no existing account is linked to the same entity.
  - Regular audits (quarterly) of the IAM system identify and resolve any duplicates.
  - Example: A contractor cannot have two accounts (e.g., jane.contractor@techsolutions.com and jane.doe@techsolutions.com) in the Online Medical Platform.

4.6 Record-Keeping of Identity Events

- **Requirement**: Records of significant events related to identity management and authentication must be maintained.
- **Implementation**:
  - The SIEM system logs all identity-related events, including:
    - Account creation, modification, or deletion.
    - Login attempts (successful and failed).
    - Permission changes.
    - Use of shared or non-human identities.
  - Logs are retained for at least 12 months to comply with GDPR, HIPAA, and ISO 27001 audit requirements.
  - Logs are reviewed monthly by the Information Security team to identify anomalies (e.g., repeated failed login attempts).
  - Example: A log entry shows that a developer accessed the customer database at 2 AM, triggering an alert for out-of-hours access.

5. Additional Security Measures

To address Tech Solutions' specific constraints and challenges:

5.1 Protection of Health Data (GDPR and HIPAA)

- Access to the customer database containing sensitive medical data is restricted to authorized roles (e.g., specific developers and customer support staff) via Role-Based Access Control (RBAC).
- MFA is mandatory for all accounts accessing the Online Medical Platform or customer database.
- Encryption (AES-256) is applied to data at rest and in transit.

5.2 Availability of Cloud Services

- Access to cloud servers is restricted to the IT Infrastructure team and approved service accounts.

- Automated monitoring ensures that access does not disrupt service availability (e.g., rate-limiting API calls).

5.3 Confidentiality of Source Code

- Access to code repositories is limited to the IT Development team and requires MFA.
- Code repositories are hosted on internal servers with strict access controls and audited regularly.

5.4 Regulatory Compliance (ISO 27001, NIS 2)

- This policy aligns with ISO 27001 Annex A controls (A.9 Access Control) and NIS 2 requirements for identity and access management.
- Annual audits ensure compliance, with findings reported to General Management.

5.5 DevSecOps

- Developers use unique identities for accessing development environments, with least privilege principles applied (e.g., read-only access for testing environments).
- Automated tools (e.g., GitLab CI/CD) enforce access controls during code deployment.

5.6 Remote Work and Mobile Devices

- Remote workers access systems via a secure VPN requiring MFA.
- Mobile Device Management (MDM) enforces security policies on devices accessing company systems.

5.7 Physical Security

- Access to physical offices and the internal data center is controlled via badge-based systems linked to employee identities.
- Only the IT Infrastructure and Information Security teams have data center access, with all entries logged.

6. Roles and Responsibilities

- **General Management**: Approves the policy and ensures resources for implementation.
- **Information Security Team**: Manages the IAM system, approves identities, monitors logs, and conducts audits.
- **HR**: Notifies the Information Security team of personnel changes (e.g., hires, departures).
- **IT Infrastructure Team**: Manages non-human identities and physical access to servers.
- **Department Heads**: Approve shared identity requests and ensure compliance within their teams.

7. Policy Enforcement

- Non-compliance (e.g., sharing passwords, using unapproved shared accounts) may result in disciplinary action, up to and including termination.
- Regular training (annually) ensures all employees understand this policy.
- The Information Security team conducts quarterly reviews to verify compliance.

8. Policy Review

- This policy is reviewed annually or upon significant changes (e.g., new regulations, infrastructure changes).
- Updates are approved by General Management and communicated to all employees.

9. Contact

For questions or to report violations, contact the Information Security team at security@techsolutions.com.

1.3 Authentication information (5.17)

Control 5.17:

Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.

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 : 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	Protect	Identity_and_ac- cess_management	Protection

Control description:

- How organizations should create, distribute, and manage passwords or PINs securely.
- When a new user is set up (e.g., during account creation), any temporary password or PIN generated automatically should be random and unique for each person.
- Users must change this temporary password the first time they log in.
- Before giving someone a new password, temporary password, or replacement, the organization must confirm they are who they claim to be (e.g., through ID checks or security questions).
- Passwords or PINs should be sent to users through secure methods (e.g., encrypted emails or secure apps), not through regular, unprotected emails.
- Users should acknowledge (e.g., via a reply or clicking a confirmation link) that they've received their password.
- Systems or software often come with default passwords set by the vendor (e.g., "admin" or "password"). These must be changed as soon as the system is installed.
- The organization should log important actions (e.g., issuing or changing passwords) and store these records securely, using approved tools like a password vault.

- Users must not share their personal passwords with anyone.
- For shared accounts (e.g., a team account), passwords should only be shared with authorized people.
- If a user suspects their password has been stolen or compromised (e.g., after a phishing attack), they must change it right away.
- Passwords should follow these best practices:
    - Don’t use personal info like names, birthdays, or phone numbers (e.g., avoid “John1985”).
    - Avoid dictionary words like “apple” or “house” (or combinations like “applehouse”).
    - Use passphrases (e.g., “SunnyHill2023!”) with letters, numbers, and special characters.
    - Ensure minimum length (usually 12+ characters for better security).
- Don’t reuse the same password across multiple services or systems
- The system should allow users to pick their own passwords and change them when needed.
- The system must ensure users create strong passwords
- When a user logs in for the first time (e.g., with a temporary password), the system must require them to set a new password.
- The system should stop users from reusing passwords they’ve used before.
- When users type their password, it should appear as dots or asterisks (e.g., ****) instead of plain text.
- Passwords should be stored and sent using encryption or hashing (approved cryptographic methods) to protect them.

Control evidence:

Checks to be performed	Evidence
➢ Whether a formal management process is implemented for the allocation of secret authentication information ➢ Whether users are required to sign an undertaking to keep secret authentication information confidential ➢ Whether temporary secret authentication information is provided to users securely ➢ If users sign an acknowledgment of receipt of secret authentication information ➢ If the default secret authentication information of the system or software vendors is changed after installation	➢ Document of the process for assigning secret authentication information ➢ Sample confidentiality commitments ➢ Sample Acknowledgments of Secret Authentication Information

TECH SOLUTIONS

PASSWORD AND ACCESS MANAGEMENT PROCEDURE

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

COPYRIGHT

Contents

1. PURPOSE

This document defines the security rules for managing passwords and access within Tech Solutions to ensure the protection of its Information Security Management System (ISMS).

2. SCOPE

This password and access management procedure applies to all components of Tech Solutions' information systems used for the creation, processing, storage, transmission, presentation, or destruction of information.

The procedure applies to:

- All departments and services of Tech Solutions.
- All users of Tech Solutions' information systems, including employees, contractors, and third parties with access.

3. INTENDED AUDIENCE

This procedure is intended for all users of Tech Solutions' information systems.

4. OWNER

This document is owned by the Information Security Management System Officer (ISMSO) of Tech Solutions.

5. VALIDITY

This procedure takes effect upon its signature by Tech Solutions' Executive Management and remains in force until further notice.

6. HANDLING EXCEPTIONS

Any deviation from this procedure must be reported and justified to the ISMSO, who reserves the right to approve or reject it.

7. GENERAL PASSWORD MANAGEMENT RULES

- **Confidentiality**: Passwords are strictly personal and must not be disclosed or shared, except with the ISMSO for specific purposes (e.g., maintenance or application testing).
- **User Awareness**: All users must be informed of their responsibility to maintain password confidentiality.
- **Compromise Reporting**: Users must immediately notify the ISMSO if they suspect their password has been compromised.

- **Initial Password Change**: Authentication mechanisms must require users to change temporary or default passwords upon first login if the password was not set by the user.
- **Secure Transmission and Storage**: Passwords must be protected during transmission and storage through:
    - Access controls and/or encryption of files containing passwords.
    - Encryption of data or communication channels during transmission.
    - Secure sealing of physical media when passwords are transmitted physically.
- **Publication of Rules**: Password creation rules must be documented and accessible to all users.
- **Default Passwords**: Vendor-supplied default passwords must be changed immediately during system or software installation.
- **Manual Entry**: Passwords must be entered manually, and automatic password memorization (e.g., in browsers or for social media) is prohibited unless approved by the ISMSO.

8. ALLOCATION AND MANAGEMENT OF AUTHENTICATION INFORMATION

This section outlines how Tech Solutions creates, distributes, and manages authentication information (e.g., passwords or PINs) securely.

- **a) Temporary Passwords/PINs Must Be Unique and Non-Guessable**
  Temporary passwords or PINs generated during user enrollment must be random, unique for each user, and changed by the user upon first login.
  Why? This prevents attackers from guessing temporary credentials and ensures only the user knows the new password.
- **b) Identity Verification**
  Before issuing new, replacement, or temporary passwords, the ISMSO must verify the user's identity (e.g., via ID checks, security questions, or multi-factor authentication).
  Why? This ensures only authorized individuals receive authentication information.
- **c) Secure Transmission**
  Passwords must be transmitted to users via secure channels (e.g., encrypted emails or secure apps). Unprotected methods, such as clear-text emails, are prohibited.
  Why? Unprotected channels can be intercepted, exposing passwords to attackers.
- **d) Acknowledgment of Receipt**
  Users must confirm receipt of authentication information (e.g., via email reply or a secure confirmation link).
  Why? This verifies that the password reached the intended recipient.
- **e) Immediate Change of Default Passwords**
  Default passwords provided by vendors (e.g., "admin" or "password") must be changed immediately upon system or software installation.
  Why? Default passwords are widely known and easily exploited.
- **f) Secure Record-Keeping**
  Records of significant events (e.g., password issuance or changes) must be logged and stored securely using approved tools (e.g., a password vault). These records must remain confidential.
  Why? This ensures traceability and protects sensitive information.

9. USER RESPONSIBILITIES

Users of Tech Solutions' information systems are responsible for maintaining the security of their authentication information.

- **a) Keep Passwords Confidential**
  Users must not share personal passwords with anyone. For shared accounts (e.g., team accounts), passwords may only be shared with authorized personnel.
  Why? Sharing passwords increases the risk of unauthorized access.
- **b) Change Compromised Passwords Immediately**
  Users must change their password immediately if they suspect it has been compromised (e.g., after a phishing attempt).
  Why? Prompt action limits potential damage from unauthorized access.
- **c) Use Strong Passwords**
  Passwords must adhere to the following best practices:
  - Avoid personal information (e.g., names, birthdays, or phone numbers).
  - Avoid dictionary words or simple combinations (e.g., "applehouse").
  - Use passphrases with a mix of uppercase, lowercase, numbers, and special characters (e.g., "SunnyHill2023!").
  - Ensure a minimum length of 12 characters for enhanced security.
    Why? Strong passwords are harder to guess or crack.
- **d) Use Unique Passwords for Each System**
  Users must not reuse passwords across different services or systems (e.g., work and personal accounts).
  Why? Reusing passwords increases the risk of multiple accounts being compromised if one is breached.
- **e) Compliance with Employment Terms**
  Adherence to these password rules is a condition of employment at Tech Solutions.
  Why? This ensures accountability and reinforces the importance of security.

10. PASSWORD MANAGEMENT SYSTEM

Tech Solutions' password management system must enforce the following requirements to ensure secure handling of authentication information.

- **a) User Control Over Passwords**
  The system must allow users to select and change their passwords, with a confirmation step (e.g., retyping the password) to prevent errors.
  Why? This empowers users and reduces input mistakes.
- **b) Enforce Strong Passwords**
  The system must enforce strong passwords as outlined in Section 9(c) (e.g., no dictionary words, minimum 12 characters).
  Why? This ensures all passwords meet high security standards.
- **c) Force Password Change at First Login**
  The system must require users to change temporary or default passwords upon first login.
  Why? This ensures only the user knows the new password.
- **d) Require Password Changes When Necessary**
  The system must enforce password changes in specific cases, such as:

- After a security incident (e.g., a data breach).
- Upon termination or role change of an employee with access to shared accounts.
  Why? This prevents the use of outdated or compromised passwords.

- **e) Prevent Password Reuse**
  The system must block users from reusing previously used passwords.
  Why? Reusing old passwords can reintroduce security risks.
- **f) Block Common or Compromised Passwords**
  The system must prevent the use of commonly used passwords (e.g., "password123") or passwords known to have been compromised in data breaches.
  Why? These passwords are easily exploited by attackers.
- **g) Mask Passwords During Entry**
  Passwords must be displayed as dots or asterisks (e.g., ****) when entered, not as plain text.
  Why? This prevents unauthorized individuals from viewing passwords.
- **h) Secure Storage and Transmission**
  Passwords must be stored and transmitted using approved cryptographic techniques (e.g., encryption or hashing).
  Why? This protects passwords from being stolen, even if a system is compromised.

11. PASSWORD CHARACTERISTICS

User Account Passwords

- Minimum length: 12 characters.
- Must not include the user's name or surname.
- Must include characters from at least three of the following categories:
  - Uppercase letters (A–Z).
  - Lowercase letters (a–z).
  - Numbers (0–9).
  - Non-alphanumeric characters (e.g., !, $, #, %).
- Password history: Must store the last 3 passwords to prevent reuse.
- Maximum lifespan: 90 days.
- Minimum lifespan: 2 days.

Privileged Account Passwords (e.g., Administrative or Service Accounts)

- Minimum length: 16 characters.
- Must include characters from at least three of the following categories:
  - Uppercase letters (A–Z).
  - Lowercase letters (a–z).
  - Numbers (0–9).
  - Non-alphanumeric characters (e.g., !, $, #, %).
- Password history: Must store the last 24 passwords to prevent reuse.
- Maximum lifespan: 42 days.
- Minimum lifespan: 1 day.

12. DOCUMENT REVISIONS

This policy will be reviewed and updated as needed by the ISMSO.

13. NON-COMPLIANCE

Any unauthorized deviation from this policy is considered a violation and may result in disciplinary action, as determined by the ISMSO.

14. RESPONSIBILITIES

The ISMSO and the ISMS team are responsible for maintaining and revising this policy.

15. DOCUMENT OWNER

The official and final version of this policy is available from the ISMSO.

16. REFERENCE DOCUMENTS

- Tech Solutions Information Security Policy.

1.5 Access rights (5.18)

Control 5.18:

Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.

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 : 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	Protect	Identity_and_ac- cess_management	Protection

Control description:

- How to grant or remove access to systems, data, or physical spaces in a secure way.
- Before giving someone access to information or assets (like files, databases, or equipment), you need approval from the person responsible for those assets. (Example: If someone needs access to a customer database, the database owner must approve it.)
- Access should only be given based on what the person needs to do their job (Example: A salesperson might need access to customer data but not to financial records)
- Ensure that the person approving access is different from the person setting it up (segregation of duties). (Example: The manager who approves access shouldn't be the one configuring the user's account.)
- Take away access rights when someone no longer needs them, especially if they leave the organization
- For temporary workers or short-term tasks, give access only for a specific time period.

- Make sure the level of access given follows the organization’s access control policies (Example: An employee shouldn’t have admin-level access if their job only requires basic user access)
- Access should only be turned on (e.g., by IT or a service provider) after all approvals are complete.
- Maintain a central list of who has access to what (e.g., a database)
- A spreadsheet or system that lists each user’s ID and what systems they can access.
- If someone changes jobs or roles within the organization, adjust their access to match their new responsibilities.
- When access is no longer needed, remove or change it by taking away keys, passwords, ID cards, or system subscriptions.(Example: If someone’s role changes, their old password or keycard should be deactivated.)
- Keep a record of any changes made to access rights, like when access is granted, changed, or removed.(Example: Log every time an employee’s access is updated in a secure system.)
- Pay special attention to users with high-level access (like admins who can change systems). (Example: Check if an IT admin still needs full system access or if it can be reduced.)
- If someone is fired, their access should be revoked immediately to prevent retaliation.
- If an employee no longer works on a project, their access to related files should be removed.

Control evidence:

Checks to be performed	Evidence
➢ If a process for provisioning or revoking physical and logical access rights granted to an entity's authenticated identity is implemented ➢ If the authorization of the owner of the information and other associated assets, for the use of this information and other associated assets, is obtained ➢ Whether the level of access granted complies with the access control policy and is compatible with other requirements such as separation of duties ➢ Whether a record of the access rights granted to a user, to access information and other associated assets, is maintained ➢ Whether the access rights of users who have changed roles or jobs are updated and whether the access rights of users who have left the organization are removed or blocked immediately ➢ Whether user access rights are reviewed at regular intervals and after any changes ➢ If user access rights are reviewed and reassigned when roles within the organization change ➢ Whether permissions for privileged access rights are reviewed at more frequent intervals	➢ Access control policy ➢ Access rights matrix

1.6 Practical Application of Clause 5.18: Case Study: ”Tech Solutions”

TECH SOLUTIONS

Tech Solutions Access Control 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 2025	Basic Document	Information Security Manager

Contents

1. Purpose

This procedure outlines the process for assigning, managing, reviewing, and revoking physical and logical access rights at Tech Solutions, in compliance with ISO/IEC 27002:2022 requirements. It ensures that access to information and assets is secure, appropriate, and aligned with business needs.

2. Scope

This procedure applies to all employees, contractors, vendors, and third parties requiring physical access to Tech Solutions facilities or logical access to systems, applications, or data.

3. Definitions

- Physical Access: Access to Tech Solutions' offices, data centers, or restricted areas.
- Logical Access: Access to IT systems, networks, applications, or data.
- Asset Owner: The individual responsible for specific information or assets (e.g., a database or server).
- Access Rights: Permissions granted to an authenticated identity to access physical or logical assets.

4. Roles and Responsibilities

- Human Resources (HR): Initiates onboarding/offboarding processes and notifies changes in employment status.
- Information Security Team: Manages logical access controls, monitors compliance,and conducts access reviews.
- Facilities Management: Manages physical access controls (e.g., keycards, biometrics).
- Asset Owners: Authorize access to their respective assets.
- Managers: Approve access requests based on business needs.
- IT Service Desk: Implements access changes after authorization.

5. Access Control Procedure

5.1 Requesting Access

1. Submit Access Request: Employees or third parties submit an access request via the Tech Solutions Access Management Portal, specifying the required physical (e.g. office access) or logical (e.g., CRM system) access.
2. Business Justification: The requester's manager provides a business justification, ensuring alignment with job responsibilities and the Access Control Policy.
3. Asset Owner Authorization: The relevant asset owner reviews and approves/denies the request based on the principle of least privilege (only necessary access is granted).
4. Management Approval: For high-risk assets (e.g., financial systems), a secondary approval from senior management is required.

5.2 Segregation of Duties

1. Separate Roles: The individual approving access (e.g., asset owner or manager) must not be the same as the individual implementing access (e.g., IT Service Desk).
2. Conflict Avoidance: Roles with conflicting duties (e.g., approving and processing payments) are not assigned to the same user. The Information Security Team verifies compliance during request reviews.

5.3 Implementing Access

1. Verification: The IT Service Desk verifies that all authorizations are complete and comply with the Access Control Policy.
2. Activation: Access is activated only after verification:
• Physical: Issue keycards or biometric registration by Facilities Management.
• Logical: Create/update user accounts, assign permissions, or issue authentication credentials (e.g., passwords, multi-factor authentication tokens).
3. Temporary Access: For contractors or temporary needs, access is granted with an expiration date (e.g., 30 days). The system automatically revokes access upon expiry.

5.4 Record Keeping

1. Central Repository: All access rights are recorded in the Access Management System, including:
• User ID (logical or physical).
• Assets accessed.
• Authorization details (approver, date).
• Expiration date (if temporary).
2. Change Log: All changes to access rights (granting, modifying, revoking) are logged with timestamps, reasons, and approvers.

5.5 Modifying Access

1. Role Changes: HR notifies the Information Security Team of role changes (e.g., promotion, department transfer). Access is adjusted to match new responsibilities.
2. Request Process: Modifications follow the same request and approval process as new access.
3. Revocation of Old Access: Unnecessary access from previous roles is revoked (e.g., removing access to marketing tools for an HR employee).

5.6 Revoking Access

1. Termination or End of Need: HR or managers notify the Information Security Team when access is no longer needed (e.g., employee termination, project completion).
2. Timely Revocation: Access is revoked within 24 hours of notification:
• Physical: Deactivate keycards, collect badges.
• Logical: Disable accounts, revoke credentials, or remove permissions.
3. Verification: The IT Service Desk confirms revocation and updates the Access Management System.

6. Review of Access Rights

1. Periodic Reviews: The Information Security Team conducts quarterly reviews of all access rights, verifying:
• Alignment with current roles and business needs.
• Removal of unnecessary access (e.g., for former projects).
• Validity of privileged access (e.g., admin accounts).
2. Event-Driven Reviews: Access is reviewed upon:
• Role changes (e.g., promotion, demotion).
• Termination of employment or contracts.
• Security incidents or policy updates.
3. Documentation: Review findings and actions (e.g., access revoked or adjusted) are logged in the Access Management System.

7. Considerations Before Employment Change or Termination

1. Risk Assessment: Before role changes or termination, the Information Security Team evaluates:
• Reason for Change: Whether the change is voluntary (e.g., resignation) or involuntary (e.g., termination), as involuntary changes may pose higher risks.
• Current Responsibilities: Whether access aligns with current duties.
• Asset Value: The sensitivity of accessible assets (e.g., customer data, intellectual property).
2. Pre-Termination Actions: For terminations:
• Access is suspended immediately upon notification.
• Physical assets (e.g., laptops, badges) are collected.
• Logical access is disabled, and credentials are reset.
3. Adjustment for Role Changes: Access is updated to reflect new responsibilities, with unnecessary access revoked.

8. Compliance and Auditing

1. Policy Alignment: All access controls comply with Tech Solutions' Access Control Policy and ISO/IEC 27002:2022.
2. Audits: The Information Security Team conducts annual audits of access records, processes, and compliance.
3. Training: Employees and managers receive annual training on access control procedures and security awareness.

9. References

• ISO/IEC 27002:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Controls.
• Tech Solutions Access Control Policy.

TECH SOLUTIONS

Access Rights Matrix

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 document defines the physical and logical access rights granted to roles within Tech Solutions, ensuring compliance with ISO/IEC 27002:2022. It serves as a centralized record to support access provisioning, review, and auditing processes.

2. Scope

This matrix applies to all employees, contractors, and third parties requiring access to Tech Solutions' facilities, systems, applications, or data.

3. Access Levels

- None: No access to the asset.
- Read: View-only access to data or systems.
- Write: Ability to modify data or configurations.
- Admin: Full control, including configuration and user management.
- Physical: Access to facilities or restricted areas.

4. Roles

- Employee (General): Standard employees (e.g., marketing, sales).
- Developer: Software engineers working on product development.
- IT Admin: Personnel managing IT infrastructure.
- HR Staff: Human Resources team managing employee data.
- Finance Staff: Personnel handling financial records.
- Manager: Department heads with approval authority.
- Contractor: Temporary workers (e.g., consultants, vendors).
- Facilities Staff: Personnel managing physical access.

5. Access Rights Matrix

Asset	Employee (General)	Developer	IT Admin	HR Staff	Finance Staff	Manager
Physical Assets						
Main Office	Physical	Physical	Physical	Physical	Physical	Physical
Data Center	None	Physical (Temp)	Physical	None	None	Physical
Restricted Areas	None	None	Physical	None	None	Physical
Logical Assets						
Employee Portal	Read	Read	Admin	Write	Read	Write
Code Repository	None	Write	Admin	None	None	Read
CRM System	Read	None	Admin	None	Read	Write
HR Database	None	None	Admin	Write	None	Read
Finance System	None	None	Admin	None	Write	Read
Network Infrastructure	None	None	Admin	None	None	None
Customer Data	Read (Limited)	None	Admin	None	Read	Write
Email System	Write	Write	Admin	Write	Write	Write

Table 1: Tech Solutions Access Rights Matrix

6. Notes

- Temporary Access: Contractors receive time-limited access (e.g., 30 days), automatically revoked upon expiration.
- Privileged Access: IT Admins hold admin-level access, subject to quarterly reviews.
- Segregation of Duties: Managers approve access; IT Admins implement it. HR and Finance Staff cannot access each other's systems.
- Least Privilege: Access is granted only as required for job functions (e.g., Employees have limited customer data access).

- Record Keeping: All access rights are logged in the Access Management System, including user IDs, assets, and approval details.
- Review Process: Access is reviewed quarterly or upon role changes/termination, ensuring alignment with current responsibilities.
- Risk-Based Adjustments: High-value assets (e.g., Finance System, Customer Data) require secondary management approval.

7. Compliance

- All access rights comply with Tech Solutions' Access Control Policy and ISO/IEC 27002:2022.
- The matrix is updated after each access review or role change and audited annually.

8. References

- ISO/IEC 27002:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Controls.
- Tech Solutions Access Control Procedure.

1.7 Information security in supplier relationships (5.19)

Control 5.19:

Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.

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 : Supplier_relation-ships_security
- 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	Identity	Supplier_relation- ships_security	Governance_and_ Ecosystem, Protec- tion

Control description:

- The organization must create a clear policy on how to work securely with suppliers
- This includes setting up processes to identify and manage risks related to the products, services, or resources (like cloud services) provided by suppliers.
- Write a specific policy about how the organization works with suppliers
- Share this policy with everyone who needs to know (e.g., employees, suppliers).
- The policy should explain how to keep information secure when using supplier products or services.
- List the kinds of suppliers you work with (e.g., IT services, logistics, utilities, banks).
- Note which suppliers could impact the confidentiality (keeping info private), integrity (ensuring info is accurate), or availability (ensuring info is accessible) of your organization's information.
- Evaluate suppliers

- Review the security measures suppliers use to protect their own systems and your information.
- Make sure their controls are accurate and complete to maintain the integrity of their services and your data.
- Clearly state which parts of your organization's information, IT systems, or physical locations (e.g., offices, data centers) suppliers can access, monitor, or control.
- Identify Risky Supplier Components: Pinpoint which supplier-provided IT components or services could affect your information's confidentiality, integrity, or availability (e.g., software, hardware, or cloud storage).
- Look for risks like: Malicious supplier employees accessing your data.
- Create plans to reduce these risks.
- Monitor Supplier Compliance: Regularly check if suppliers follow your security requirements.
- Handle Non-Compliance: If a supplier doesn't meet security standards, take action to fix the issue (e.g., work with them to improve or switch suppliers).
- Manage Incidents: Have a plan for handling problems with supplier products or services (e.g., a software failure or data breach).
- Define who (you or the supplier) is responsible for fixing issues.
- When stopping work with a supplier, ensure: Their access to your systems is removed.
- Plan for Supplier Failure: Have backup plans, like identifying alternative suppliers in advance, to avoid delays.

Control evidence:

Checks to be performed	Evidence
➢ If a policy identifying and imposing specific security measures on supplier access to assets ➢ Whether processes and procedures to address security risks associated with the use of vendor products and services are identified ➢ Whether the types of suppliers to whom the organization will grant access to its information are identified and documented ➢ Whether the supplier evaluation and selection criteria are defined and documented ➢ If we contractually impose on any supplier who may have access to sensitive information, compliance with security clauses ➢ If an analysis of the risks linked to access by the supplier's personnel to the information system or to premises containing information is carried out and if the necessary security measures are defined accordingly ➢ Whether the types of access to information that different types of suppliers will be granted are defined and whether this access is monitored and controlled ➢ Whether incidents associated with supplier access, including the responsibilities of the organization and those of the suppliers, are identified and addressed	➢ Policy identifying and imposing specific security measures on supplier access to assets ➢ List of supplier types (e.g. IT services, logistics services, financial services) ➢ Commitments to respect security clauses signed by the supplier's employees ➢ Risk analysis report relating to access by supplier personnel ➢ List of types of access to information granted to different types of suppliers ➢ Incident processing report and associated supplier access

1.8 Practical Application of Clause 5.19: Case Study: ”Tech Solutions”

TECH SOLUTIONS

Supplier Security 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 2015	Basic Document	Information Security Manager

Contents

1. Purpose

This policy establishes security measures to manage relationships with suppliers accessing Tech Solutions' information assets or providing products and services. It aims to protect the confidentiality, integrity, and availability of information by:

- Mitigating risks of malicious or inappropriate actions by suppliers.
- Ensuring suppliers comply with security requirements.
- Maintaining a consistent security level for outsourced or subcontracted services.

2. Scope

This policy applies to all suppliers providing products or services to Tech Solutions, including cloud service providers, IT vendors, logistics, utilities, and financial services. It covers all employees, contractors, and third parties interacting with suppliers.

3. Supplier Identification

Tech Solutions will identify and document supplier types that may impact the confidentiality, integrity, or availability of information, including:

- **ICT Services**: Software providers, cloud storage, IT support.
- **Logistics**: Transportation and delivery services.
- **Utilities**: Electricity and internet providers.
- **Financial Services**: Payment processors, banks.
- **ICT Infrastructure**: Hardware and network component vendors.

4. Supplier Evaluation and Selection

Suppliers will be evaluated based on the sensitivity of information, products, or services involved, using:

- **Market Analysis**: Reviewing reputation and customer references.
- **Certifications**: Verifying standards (e.g., ISO 27001).
- **On-Site Assessments**: Inspecting critical facilities.
- **Document Review**: Analyzing security policies and controls. Only suppliers with robust security controls will be selected. Evaluations will be documented using a standardized template (see Appendix).

5. Supplier Security Controls

Tech Solutions will review the accuracy and completeness of suppliers' security controls, ensuring:

- Protection against vulnerabilities (e.g., regular patching).
- Secure handling of data processed or stored by the supplier. Reviews will occur before contract signing and annually thereafter.

6. Supplier Access Control

Tech Solutions will define and document what suppliers can access, monitor, or control, including:

- **Information**: Specific datasets (e.g., customer databases).
- **ICT Services**: Systems (e.g., servers, applications).
- **Physical Infrastructure**: Offices, data centers. Access will be restricted to the minimum necessary, using named accounts and activity logging.

7. Risk Assessment and Management

Tech Solutions will assess risks associated with suppliers, including:

- **Asset Misuse**: Risks from unauthorized use or malicious personnel.
- **Product Vulnerabilities**: Software or hardware flaws (e.g., bugs, exploits). Mitigation plans will include:
- Background checks for supplier personnel.
- Regular testing of supplier products for vulnerabilities. Risks will be reassessed annually or after incidents.

8. Security Oversight Committee

A Security Oversight Committee will:

- Monitor supplier compliance with security requirements.
- Manage incidents and recommend improvements.
- Validate security asset transfers during termination. The committee will meet quarterly and document findings.

9. Compliance Monitoring

Supplier compliance will be monitored through:

- **Third-Party Audits**: Independent security assessments.
- **Product Validation**: Testing software/hardware security.
- **Periodic Reports**: Performance indicators from suppliers. Non-compliance will trigger a 30-day correction period, with escalation to contract suspension if unresolved.

10. Incident and Contingency Management

Tech Solutions will maintain an incident response plan for supplier-related issues, defining:

- **Responsibilities**:
  - Tech Solutions: Investigate and mitigate internal impacts.
  - Supplier: Address issues with their products/services.
- **Process**: 24-hour notification, root cause analysis, corrective actions. Contingency plans will include temporary solutions (e.g., switching to an alternate supplier).

11. Resilience and Recovery

To ensure information availability, Tech Solutions will:

- Identify alternate suppliers for critical services.
- Maintain and test recovery plans annually.
- Ensure regular backups of supplier-hosted data.

12. Staff Training

Employees interacting with suppliers will receive training on:

- This policy and related procedures.
- Secure interaction with supplier personnel.
- Behavior based on supplier access levels. Training will occur at onboarding and annually.

13. Supplier Obligations

Suppliers must:

- Notify Tech Solutions of risks, incidents, or performance degradation.
- Maintain state-of-the-art security mechanisms.
- Report operations that may impact system availability.

14. Regulatory and Legal Compliance

Suppliers must comply with:

- Data protection laws (e.g., GDPR).
- Non-disclosure agreements (NDAs).
- Intellectual property rights.
- Local regulations at their operational sites. Compliance will be verified through regular audits.

15. Supplier Personnel Security

Suppliers will provide:

- An updated list of authorized personnel with access levels.
- Background checks and qualifications for employees.
- Regular information security training. Tech Solutions will validate these measures during evaluations.

16. Physical Security of Supplier Facilities

Suppliers must maintain:

- Physical access controls (e.g., badges, cameras).
- Secure environments for data centers or offices. Tech Solutions will inspect critical facilities before contracting.

17. Maintenance and Support Interventions

External maintenance or support personnel will:

- Be accompanied by an authorized Tech Solutions employee.
- Use designated accounts for traceable actions. Storage media (e.g., hard drives) remain Tech Solutions' property and will be erased or destroyed in the presence of a representative.

18. Confidentiality

Suppliers will sign confidentiality agreements covering:

- Hosted data and sensitive information (e.g., passwords, encryption keys).
- Ongoing obligations post-contract termination. Breaches will result in contractual penalties.

19. System Transfers

During data or system transfers, suppliers will ensure:

- Integrity and confidentiality via secure backups.
- Use of encrypted channels (e.g., HTTPS, SFTP). Transfers will be documented and verified.

20. Data Localization

Suppliers will provide a list of data storage locations (e.g., primary sites, backup sites). Post-incident, they will identify affected data locations.

21. Service Level Agreements (SLAs)

Suppliers will adhere to SLAs, including:

- Availability rate (e.g., 99.9%).
- Maximum monthly downtime.
- Guaranteed intervention (GTI) and restoration (GTR) times. Penalties for non-compliance will be contractually defined.
-

22. Application Development Security

Suppliers will ensure secure development, following:

- OWASP guidelines for web applications.
- Least privilege principles.
- Pre-deployment code reviews. Detected issues will be corrected at the supplier's expense.

23. Operational Security

Operational procedures will be:

- Documented and restricted to authorized personnel.
- Updated to reflect security requirements. Asset responsibilities will be clearly defined.

24. Change Management

Changes (e.g., updates, upgrades) will be:

- Verified for security compliance.
- Approved by Tech Solutions before implementation.

25. Workstation Security

Supplier workstations will be secured with:

- Named user authentication.
- Regular updates and antivirus software.
- Annual application inventory to detect unauthorized software. Sensitive data will follow Tech Solutions' classification policy.

26. Termination and Reversibility

Upon termination, suppliers will:

- **De-Provision Access**: Remove all accounts and permissions.
- **Handle Information**: Return, transfer, or securely delete data.
- **Intellectual Property**: Clarify ownership of developed assets.
- **Data Portability**: Enable transfer to a new supplier or in-house.
- **Records Management**: Retain required records per legal obligations.
- **Asset Return**: Return physical equipment.
- **Secure Disposal**: Erase data using certified tools, witnessed by Tech Solutions.
- **Ongoing Confidentiality**: Adhere to NDAs post-termination. Suppliers will assist during transition, including:
- Training the new supplier.
- Transferring technical documentation.
- Two-week operational observation period.

27. Continuity Planning

To address supplier unavailability (e.g., bankruptcy, service discontinuation), Tech Solutions will:

- Identify alternate suppliers in advance.
- Maintain contracts with multiple suppliers for critical services.
- Document replacement procedures.

28. Cloud Service Providers

For cloud providers, Tech Solutions will:

- Evaluate specific security controls (e.g., encryption, access management).
- Monitor performance and compliance via regular audits.
- Ensure data portability for supplier changes.

29. Contract Termination

For significant security breaches, Tech Solutions will:

- Issue a 30-day notice to remedy the issue.
- Terminate the contract if non-compliance persists. Penalties for violations will be contractually defined.

30. Non-Compliance

Unauthorized deviations from this policy will be treated as violations, leading to:

- Disciplinary action for employees.
- Contract termination for suppliers. Violations must be reported to the CISO immediately.

31. Policy Review

This policy will be reviewed annually or upon significant changes (e.g., new regulations). The CISO oversees the review process.

32. Responsibilities

- **CISO**: Oversees policy implementation, review, and compliance.
- **Procurement Team**: Ensures compliant supplier selection.
- **Employees**: Adhere to the policy when interacting with suppliers.
- **Suppliers**: Comply with security requirements and report incidents promptly.

TECH SOLUTIONS

List of Suppliers

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 2018	Basic Document	Information Security Manager

Contents

1. Purpose

This document provides a comprehensive list of suppliers engaged by Tech Solutions, detailing their roles, security profiles, and compliance status to ensure alignment with ISO 27002 requirements. It supports the secure management of supplier relationships by identifying risks, access levels, and security controls, protecting the confidentiality, integrity, and availability of Tech Solutions' information assets.

2. Scope

This document covers all suppliers providing products or services to Tech Solutions, including cloud service providers, IT vendors, logistics, utilities, and financial services. It is intended for use by the procurement team, information security team, and other relevant stakeholders.

3. Compliance with ISO 27002

The List of Suppliers addresses the following ISO 27002 requirements:

- **Supplier Identification**: Categorizing suppliers based on their potential impact on information security (e.g., ICT, logistics).
- **Evaluation and Selection**: Documenting evaluation criteria and security control assessments.
- **Access Control**: Specifying what information, systems, or facilities suppliers can access.
- **Risk Assessment**: Identifying risks associated with supplier products, services, or personnel.
- **Compliance Monitoring**: Tracking adherence to security requirements.
- **Termination Procedures**: Ensuring secure handling of assets and data upon contract termination.
- **Cloud Service Providers**: Including specific considerations for cloud-based suppliers.

4. Supplier List Overview

The table below lists all active suppliers, providing key details to manage their security impact. Each entry includes:

- **Supplier Name and Type**: Name and category (e.g., ICT Services, Logistics).
- **Contact Information**: Primary contact for communication.
- **Services/Products Provided**: Description of deliverables.
- **Impact on CIA**: Potential impact on Confidentiality, Integrity, Availability.
- **Evaluation Status**: Results of security evaluations (e.g., certifications, audits).
- **Access Levels**: Information, systems, or facilities accessible to the supplier.
- **Risk Assessment**: Identified risks and mitigation measures.
- **Compliance Status**: Adherence to security policies and SLAs.
- **Last Review Date**: Date of the most recent compliance review.

5. Supplier List

Supplier Name	Type	Contact	Services/Products	Impact on CIA	Evaluation Status	Access Levels	Risk Assessment	Compliance Status	Last Review Date
CloudTech Inc.	Services (Cloud)	jane@cloudtech.com, +1-555-1234	Cloud storage and computing services	High (Confidentiality, Availability)	ISO 27001 certified, on-site audit passed (Jan 2025)	Customer database	Risk: Data breach due to misconfiguration. Mitigation: Encrypted storage, regular audits.	Compliant	Apr 2025
NetSecure	ICT Services	john@netsecure.com, +1-555-5678	Cybersecurity software and support	Medium (Integrity, Availability)	SOC 2 compliant	dashboards, network logs	Risk: Software vulnerabilities. Mitigation: Monthly patch updates, penetration testing.	Compliant	Mar 2025
FastLogistics	Logistics	sarah@fastlogistics.com, +1-555-9012	Delivery of hardware components	Low (Availability)	no certifications	Warehouse access	Risk: Physical theft. Mitigation: GPS tracking, escorted access.	Compliant	Feb 2025
PowerGrid Co.	Utilities	mike@powergrid.com, +1-555-3456	Electricity supply for data centers	High (Availability)	SLA verified	Data center power infrastructure	Risk: Power outage. Mitigation: Backup generators, alternate provider identified.	Compliant (100% uptime)	Apr 2025
PaySafe Solutions	Financial Services	emily@paysafe.com, +1-555-7890	Payment processing	High (Confidentiality, Integrity)	PCI DSS compliant	. Payment transaction data	Risk: Fraudulent transactions. Mitigation: Multi-factor authentication, transaction monitoring	Compliant	Mar 2025

6. Procedures for Maintaining the Supplier List

To ensure the list remains accurate and compliant with ISO 27002:

- **Updates**: The procurement and security teams will update the list quarterly or upon onboarding/terminating a supplier.
- **Reviews**: The Security Oversight Committee will review each supplier's compliance annually, updating evaluation and risk assessment details.
- **Risk Assessments**: Conducted before onboarding and annually, with results documented in the list.
- **Access Control**: Access levels will be validated during reviews to ensure minimal access is granted.
- **Termination Planning**: Termination plans will be tested during annual security drills to ensure secure asset handling.

7. Responsibilities

- **Chief Information Security Officer (CISO)**: Oversees the maintenance and compliance of the supplier list.
- **Procurement Team**: Updates supplier details and coordinates evaluations.
- **Security Team**: Conducts risk assessments and compliance audits.
- **Suppliers**: Provide required documentation (e.g., certifications, SLAs) and report incidents promptly.

8. Compliance Monitoring

- **Audits**: Third-party audits or internal reviews will verify supplier security controls annually.
- **SLA Tracking**: Monthly performance reports will be compared against SLAs.
- **Incident Reporting**: Suppliers must report security incidents within 24 hours, with details logged in the supplier list.

9. Termination and Reversibility

For each supplier, the termination plan ensures:

- **Access De-Provisioning**: Immediate removal of all system and physical access.
- **Data Handling**: Return, transfer, or secure deletion of data, witnessed by Tech Solutions.
- **Intellectual Property**: Ownership clarification for developed assets.
- **Data Portability**: Transfer of data to a new supplier or in-house systems.
- **Asset Return**: Return of physical assets (e.g., hardware).
- **Secure Disposal**: Certified data destruction with documentation.
- **Ongoing Confidentiality**: Enforcement of NDAs post-termination.

TECH SOLUTIONS

Supplier Employee Security Commitment

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 document outlines the security commitments that employees of suppliers engaged by Tech Solutions must adhere to, ensuring the protection of Tech Solutions' information assets. By signing this commitment, supplier employees acknowledge their responsibility to comply with Tech Solutions' security clauses, to safeguard the confidentiality, integrity, and availability of information.

2. Scope

This commitment applies to all employees, contractors, or agents of suppliers who access Tech Solutions' information, systems, or facilities, including those working for cloud service providers, IT vendors, logistics, utilities, or financial services. It is a condition of engagement with Tech Solutions.

3. Requirements

This commitment addresses the following requirements:

- **Personnel Security**: Ensuring supplier employees are trained to handle sensitive information securely.
- **Confidentiality**: Enforcing non-disclosure obligations during and after engagement.
- **Access Control**: Restricting access to authorized systems and information.
- **Incident Management**: Requiring prompt reporting of security incidents.
- **Compliance Monitoring**: Allowing Tech Solutions to audit adherence to security obligations.
- **Termination Procedures**: Ensuring secure handling of assets and data upon cessation of access.

4. Security Commitments

As an employee of a supplier working with Tech Solutions, I commit to the following security obligations:

4.1. Confidentiality

- I will not disclose, share, or misuse any confidential information belonging to Tech Solutions, including customer data, system configurations, passwords, or encryption keys, unless explicitly authorized.
- I will adhere to the terms of any non-disclosure agreement (NDA) signed with Tech Solutions, and this obligation will continue after my engagement ends.
- I will use confidential information only for the purposes specified in my role and will not copy, transfer, or store it on unauthorized devices or systems.

4.2. Access Control

- I will access only the information, systems, or facilities explicitly authorized by Tech Solutions, as defined in my role.
- I will use named accounts provided by Tech Solutions or my employer for all access and will not share credentials with others.
- I will immediately report any unauthorized access attempts or suspicious activity to my supervisor and Tech Solutions' Information Security Team.

4.3. Secure Handling of Assets

- I will protect physical and digital assets provided by Tech Solutions, such as hardware, storage media, or documents, from loss, theft, or damage.
- I will not remove, modify, or dispose of Tech Solutions' assets without prior authorization.
- I will ensure that any storage media (e.g., USB drives, hard drives) containing Tech Solutions' data are securely stored and returned or destroyed as instructed.

4.4. Incident Reporting

- I will report any security incidents, such as data breaches, system malfunctions, or policy violations, to my supervisor and Tech Solutions' Information Security Team (security@techsolutions.com) within 24 hours.
- I will cooperate fully with investigations into security incidents, providing accurate and timely information as requested.

4.5. Compliance with Security Policies

- I will comply with Tech Solutions' Supplier Relationship Security Policy and any related procedures communicated to me or my employer.
- I will participate in security training provided by my employer or Tech Solutions, as required, to understand my responsibilities.
- I will adhere to all applicable laws, regulations, and contractual obligations, including data protection laws (e.g., GDPR) and intellectual property rights.

4.6. Secure Workstation Practices

- I will ensure that workstations or devices used to access Tech Solutions' systems are secured with up-then I will not store sensitive Tech Solutions' data on personal or unauthorized devices.

4.7. Termination and Reversibility

- Upon termination of my engagement or access to Tech Solutions' systems, I will:
    - Immediately cease accessing Tech Solutions' information, systems, or facilities.
    - Return all physical assets (e.g., hardware, access badges) to my employer or Tech Solutions.

    - Cooperate in the secure deletion or transfer of any Tech Solutions' data in my possession, as witnessed by Tech Solutions.
    - Maintain confidentiality obligations post-termination, as per the NDA.
- I understand that Tech Solutions may revoke my access at any time, and I will comply with all termination procedures.

4.8. Physical Security

- I will adhere to physical security requirements at Tech Solutions' facilities or supplier sites, such as using access badges, following escorted access protocols, and respecting restricted areas.
- I will report any physical security breaches (e.g., unauthorized entry) immediately.

5. Responsibilities

- **Supplier Employee**: I am responsible for understanding and adhering to these commitments, reporting incidents, and cooperating with Tech Solutions' security measures.
- **Supplier Employer**: My employer will ensure I receive necessary training, provide authorized access credentials, and communicate Tech Solutions' security requirements.
- **Tech Solutions**: The Information Security Team will monitor compliance, provide guidance, and enforce these commitments through audits and access controls.

6. Compliance Monitoring

- Tech Solutions may audit my adherence to these commitments through access logs, incident reports, or third-party reviews.
- I agree to provide documentation or evidence of compliance (e.g., training completion) upon request.
- Non-compliance may result in disciplinary action by my employer, revocation of access, or legal consequences, as determined by Tech Solutions.

7. Acknowledgment and Signature

I, the undersigned, acknowledge that I have read, understood, and agree to comply with the security commitments outlined in this document. I understand that failure to adhere to these commitments may result in disciplinary action, termination of access, or legal consequences. I commit to protecting Tech Solutions' information assets.

Name: _____
Position: _____
Supplier Name: _____
Date: _____
Signature: _____

Tech Solutions Representative:
Name: _____
Position: Information Security Officer
Date: _____
Signature: _____

8. Contact

For questions or to report incidents, contact the Tech Solutions Information Security Team at security@techsolutions.com.

1.9 Addressing information security within supplier agreements (5.20)

Control 5.20:

Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.

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 : Supplier_relation-ships_security
- 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	Identity	Supplier_relation- ships_security	Governance_and_ Ecosystem, Protec- tion

Control description:

- Describe what information the supplier will access or receive (e.g., customer data, financial records).
- Specify how this information will be shared or accessed (e.g., via email, cloud platform, or physical documents)
- List all laws, regulations, and contracts the supplier must follow (e.g., data protection laws like GDPR, intellectual property rules).
- Explain how the supplier will comply with these requirements. (Example: If handling personal data, the supplier must follow privacy laws and prove compliance.)
- The supplier must follow your organization's security policies (Example: Require the supplier to use strong passwords and report security incidents.)
- Define acceptable and unacceptable ways to use the information or assets (Example: A supplier can't share your data with others without permission.)

- Set minimum security standards for the supplier's IT systems based on the type of information and access (Example: Require encryption for sensitive data stored on their servers.)
- Include terms for compensation or fixes if the supplier fails to meet security requirements. (Example: If a breach occurs due to their negligence, they cover the costs.)
- Define how the supplier should handle security incidents (Example: If there's a data breach, they must report it immediately and work with you to resolve it.)
- Require the supplier to train their staff on your security policies and procedures. (Example: Train their team on how to spot phishing emails.)
- Name a specific person at the supplier's organization for security-related questions or issues.
- Where legally allowed, require background checks for supplier employees handling your information (Example: Ensure their staff are vetted before accessing sensitive data.)
- Ask for evidence (e.g., certifications, audit reports) that the supplier meets security standards. (Example: Request a SOC 2 report to verify their security controls.)
- Reserve the right to audit the supplier's processes and controls to ensure compliance. (Example: Conduct annual checks of their security practices.)
- Require the supplier to provide periodic reports on their security controls and fix any issues quickly. (Example: Submit a quarterly report on firewall performance.)
- Define processes for fixing problems (e.g., bugs in their system)
- Ensure the supplier backs up your data according to your needs (e.g., frequency, storage location). (Example: Daily backups stored in a secure, offsite location.)
- Require the supplier to notify you of changes (e.g., system updates) and allow you to reject them if needed. (Example: Inform you before upgrading software that handles your data.)
- Include terms for ending the contract, such as returning assets, securely disposing of data, and maintaining confidentiality afterward. (Example: Return all customer data and destroy copies when the contract ends.)
- Ensure the supplier securely deletes your information when it's no longer needed. (Example: Shred physical documents or wipe digital data permanently.)
-

Control evidence:

Checks to be performed	Evidence
➢ If an agreement signed with a third party involving access to the information system or to the premises containing information is defined and documented ➢ Whether agreements with suppliers contain compliance with all information security requirements (including description and classification of information, methods of accessing information and rules for acceptable use of information ➢ Whether agreements with suppliers contain legal, statutory, regulatory and contractual requirements, including data protection, processing of personal data (PD), intellectual property rights and copyright ➢ Whether agreements with suppliers contain incident management requirements (in particular notification and collaboration during corrective action) ➢ Whether the agreements with suppliers contain security measures for the transfer of information ➢ If any access by a third party to the information system or to the premises containing information is only authorized after the signing of a formal agreement containing these clauses.	➢ Document defining all the security clauses that any agreement signed with a third party should include

1.10 Practical Application of Clause 5.20: Case Study: ”Tech Solutions”

TECH SOLUTIONS

Tech Solutions Supplier Agreement

Purpose

This document provides practical examples to illustrate how Tech Solutions implements the ISO 27002 supplier agreement requirements in its supplier relationships. These examples are designed to help beginners understand how the **Tech Solutions Supplier Agreement Procedure** is applied in real-world scenarios.

Scope

The examples cover all ISO 27002 supplier agreement requirements (a–z) and are tailored to Tech Solutions, a technology organization that develops software and manages customer data. The examples involve a fictional supplier, **CloudSecure**, which provides cloud hosting services to Tech Solutions.

Context

- **Tech Solutions**: A software company that handles sensitive customer data (e.g., personal information, financial records) and proprietary code.
- **CloudSecure**: A cloud service provider hosting Tech Solutions' customer data and application servers.
- **Scenario**: Tech Solutions is drafting a supplier agreement with CloudSecure to ensure compliance with ISO 27002 and protect its information assets.

Examples

1. Information Description and Access Methods (a)

- **Requirement**: Specify the information to be provided or accessed and methods of access.
- **Example**:
  Agreement Excerpt: "CloudSecure will host Tech Solutions' customer database, including names, email addresses, and transaction histories. Access will be provided via a secure API with OAuth 2.0 authentication and TLS 1.3 encryption. Physical access to servers is prohibited."
  Scenario: Tech Solutions ensures CloudSecure only accesses the customer database through a predefined, secure API, reducing the risk of unauthorized access.

2. Information Classification (b)

- **Requirement**: Classify information per Tech Solutions' classification scheme.
- **Example**:
  Agreement Excerpt: "All customer data hosted by CloudSecure is classified as 'Confidential' per Tech Solutions' Information Classification Policy. Data must be labeled as 'Confidential' in all storage and processing systems."

Scenario: CloudSecure tags the customer database with a "Confidential" label in its system, ensuring appropriate handling (e.g., encryption, restricted access).

3. Classification Mapping (c)

- **Requirement**: Map Tech Solutions' classification scheme to the supplier's scheme.
- **Example**:
  Agreement Excerpt: "Tech Solutions' 'Confidential' classification corresponds to CloudSecure's 'Restricted' category. CloudSecure will treat all 'Confidential' data as 'Restricted' and apply equivalent security controls."
  Scenario: During contract negotiations, Tech Solutions and CloudSecure create a mapping table to align their classification terms, avoiding miscommunication.

4. Legal and Regulatory Requirements (d)

- **Requirement**: List legal, statutory, regulatory, and contractual requirements.
- **Example**:
  Agreement Excerpt: "CloudSecure will comply with GDPR for EU customer data and CCPA for California residents. Compliance will be demonstrated through annual third-party audits and submission of a GDPR Data Processing Agreement."
  Scenario: CloudSecure signs a GDPR DPA and provides an audit report to prove compliance, satisfying Tech Solutions' legal obligations.

5. Security Controls (e)

- **Requirement**: Agree on controls, including access control, monitoring, and auditing.
- **Example**:
  Agreement Excerpt: "CloudSecure will implement role-based access control (RBAC) for its staff, use intrusion detection systems, and submit quarterly audit logs to Tech Solutions. CloudSecure will comply with Tech Solutions' Information Security Policy."
  Scenario: CloudSecure restricts database access to three authorized engineers and provides Tech Solutions with logs showing access attempts.

6. Acceptable Use (f)

- **Requirement**: Define acceptable and unacceptable use of information and assets.
- **Example**:
  Agreement Excerpt: "CloudSecure may use customer data only for hosting and maintenance purposes. Sharing data with third parties or using it for analytics is prohibited."
  Scenario: CloudSecure is barred from using Tech Solutions' data for its own marketing, ensuring data privacy.

7. Personnel Authorization (g)

- **Requirement**: Specify procedures for authorizing and removing supplier personnel access.
- **Example**:
  Agreement Excerpt: "CloudSecure will provide a list of personnel authorized to access Tech Solutions' data, updated quarterly. Access will be revoked within 24 hours of an employee's departure."
  Scenario: CloudSecure submits a list of five engineers with access and notifies Tech Solutions when one leaves, ensuring only authorized staff access data.

8. Supplier ICT Infrastructure (h)

- **Requirement**: Set minimum security standards for the supplier's IT infrastructure.
- **Example**:
  Agreement Excerpt: "CloudSecure's servers will use AES-256 encryption for data at rest and maintain up-to-date antivirus software. Firewalls must block unauthorized IP addresses."
  Scenario: CloudSecure configures its servers to meet Tech Solutions' encryption standards, protecting customer data from breaches.

9. Indemnities and Remediation (i)

- **Requirement**: Include terms for compensation or fixes for non-compliance.
- **Example**:
  Agreement Excerpt: "CloudSecure will indemnify Tech Solutions for losses caused by data breaches due to CloudSecure's negligence, including legal fees and remediation costs."
  Scenario: If a breach occurs because CloudSecure failed to patch a server, they cover Tech Solutions' costs for notifying affected customers.

10. Incident Management (j)

- **Requirement**: Define incident management procedures, including notification.
- **Example**:
  Agreement Excerpt: "CloudSecure will notify Tech Solutions within 24 hours of detecting a security incident and provide a detailed report within 72 hours. CloudSecure will collaborate on remediation efforts."
  Scenario: When CloudSecure detects a phishing attack, they notify Tech Solutions immediately and work together to isolate affected systems.

11. Training and Awareness (k)

- **Requirement**: Require training on security procedures.
- **Example**:
  Agreement Excerpt: "CloudSecure's staff will complete Tech Solutions' annual security awareness training, covering phishing, incident response, and data handling."
  Scenario: CloudSecure's engineers complete a 1-hour online training module provided by Tech Solutions, improving their security practices.

12. Subcontracting (l)

- **Requirement**: Ensure subcontractors follow the same security obligations.
- **Example**:
  Agreement Excerpt: "CloudSecure must obtain written approval from Tech Solutions before using subcontractors. Subcontractors must sign agreements mirroring this contract's security terms."
  Scenario: CloudSecure seeks approval to use a backup provider, ensuring they meet Tech Solutions' security standards.

13. Contact Persons (m)

- **Requirement**: Designate a contact for security issues.
- **Example**:
  Agreement Excerpt: "CloudSecure's Security Officer, Jane Doe (jane.doe@cloudsecure.com), will be the primary contact for security matters."
  Scenario: Tech Solutions contacts Jane Doe directly when reviewing audit logs, streamlining communication.

14. Personnel Screening (n)

- **Requirement**: Require background checks for supplier personnel (where legally permissible).
- **Example**:
  Agreement Excerpt: "CloudSecure will conduct background checks on all personnel accessing Tech Solutions' data and notify Tech Solutions of any concerns within 48 hours."
  Scenario: CloudSecure verifies that its engineers have no criminal records, providing Tech Solutions with assurance.

15. Assurance Mechanisms (o)

- **Requirement**: Require evidence of compliance (e.g., certifications).
- **Example**:
  Agreement Excerpt: "CloudSecure will provide an annual SOC 2 Type II report and ISO 27001 certification to demonstrate compliance with security standards."
  Scenario: CloudSecure submits its SOC 2 report, which Tech Solutions reviews to confirm robust controls.

16. Right to Audit (p)

- **Requirement**: Reserve the right to audit supplier processes.
- **Example**:
  Agreement Excerpt: "Tech Solutions may conduct annual on-site audits of CloudSecure's data centers with 30 days' notice to verify compliance."
  Scenario: Tech Solutions schedules an audit to inspect CloudSecure's server security, ensuring adherence to the agreement.

17. Effectiveness Reports (q)

- **Requirement**: Require periodic reports on control effectiveness.
- **Example**:
  Agreement Excerpt: "CloudSecure will submit quarterly reports on firewall performance and patch management, addressing issues within 30 days."
  Scenario: CloudSecure's report shows a missed patch, which they fix within the agreed timeline.

18. Defect and Conflict Resolution (r)

- **Requirement**: Define processes for resolving defects or disputes.
- **Example**:
  Agreement Excerpt: "Security defects must be resolved within 14 days. Unresolved disputes will be escalated to senior management of both parties."
  Scenario: When CloudSecure delays fixing a vulnerability, Tech Solutions escalates the issue, prompting quick resolution.

19. Backups (s)

- **Requirement**: Specify backup frequency, type, and storage.
- **Example**:
  Agreement Excerpt: "CloudSecure will perform daily backups of Tech Solutions' data, stored in an encrypted, offsite facility in a different region."
  Scenario: CloudSecure maintains nightly backups, ensuring data recovery in case of a server failure.

20. Disaster Recovery (t)

- **Requirement**: Require an alternate facility and fallback controls.
- **Example**:
  Agreement Excerpt: "CloudSecure will maintain a disaster recovery site in a separate geographic region, with failover capabilities activated within 4 hours of a primary site failure."
  Scenario: During a regional outage, CloudSecure switches to its backup site, maintaining service availability.

21. Change Management (u)

- **Requirement**: Require notification of changes and the option to reject them.
- **Example**:
  Agreement Excerpt: "CloudSecure will notify Tech Solutions 30 days before software updates. Tech Solutions may reject updates that pose security risks."
  Scenario: CloudSecure proposes a server upgrade, but Tech Solutions delays it until compatibility is verified.

22. Physical Security (v)

- **Requirement**: Ensure physical security matches information classification.
- **Example**:
  Agreement Excerpt: "CloudSecure's data centers will use biometric access controls and 24/7 CCTV to protect 'Confidential' data."
  Scenario: CloudSecure's facility restricts access to authorized personnel, safeguarding Tech Solutions' data.

23. Information Transfer (w)

- **Requirement**: Protect information during transfer.
- **Example**:
  Agreement Excerpt: "Data transfers between CloudSecure and Tech Solutions will use SFTP with AES-256 encryption."
  Scenario: CloudSecure securely transfers backup files to Tech Solutions, preventing interception.

24. Termination Clauses (x)

- **Requirement**: Define obligations upon contract termination.
- **Example**:
  Agreement Excerpt: "Upon termination, CloudSecure will return all data to Tech Solutions within 7 days, destroy copies, and maintain confidentiality indefinitely."
  Scenario: When the contract ends, CloudSecure returns data and provides a certificate of destruction.

25. Secure Data Destruction (y)

- **Requirement**: Ensure secure deletion of information.
- **Example**:
  Agreement Excerpt: "CloudSecure will use NIST 800-88-compliant methods to wipe Tech Solutions' data from its systems when no longer needed."
  Scenario: CloudSecure securely erases old backups, ensuring no residual data remains.

26. Handover Support (z)

- **Requirement**: Provide support for transferring data or services.
- **Example**:
  Agreement Excerpt: "CloudSecure will provide Tech Solutions' data in CSV format within 14 days to support handover to a new provider."
  Scenario: CloudSecure exports the customer database in a usable format, enabling a smooth transition to a new supplier.

Notes for Implementation

- **Beginner Tip**: Use these examples as a checklist when drafting agreements. Start with the most critical terms (e.g., legal requirements, incident management) and expand as needed.
- **Customization**: Adjust terms based on the supplier's role (e.g., a software developer may need different controls than a cloud provider).
- **Verification**: Always verify supplier compliance through audits, reports, or certifications, as shown in the examples.