Noureddine Kangari

ISO/IEC 27002:2022

Master the Essentials of Information Security Controls

Your Path to Achieving ISO/IEC 27001 Certification

Learn How to Avoid Minor and Major Non-Conformities

PART 6

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 Information security during disruption (5.29)

Control 5.29:

The organization should plan how to maintain information security at an appropriate level during disruption.

Control attributes:

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

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventive, Corrective	Confidentiality Integrity Availability	Protect, Respond	Continuity	Protection Resilience

Control description:

- Decide what security is needed to protect critical information if your business faces a disruption, like a server crash or a ransomware attack. (Example: The retail business relies on its website to process customer orders and store payment details. If the website goes down, the business needs to ensure customer data (like credit card info) remains secure. They decide that encryption and access controls must stay active, even during a disruption, to prevent data theft.)
- Make sure your plans to keep the business running (business continuity plans) include steps to protect information security. (Example: The business has a business continuity plan that says, “If our website server fails, we’ll switch to a backup server within 4 hours.” They add security steps to this plan, like: “The backup server must have the same firewall and encryption as the main server to protect customer data.”)
- Create detailed plans to maintain or restore security during a disruption, test them to make sure they work, and review them regularly to improve. (Example: The business creates a plan to restore its website after a cyberattack. The plan includes restoring data from a secure backup and ensuring only authorized staff can access it. They test this plan by simulating a cyberattack to see if the backup works and if data stays

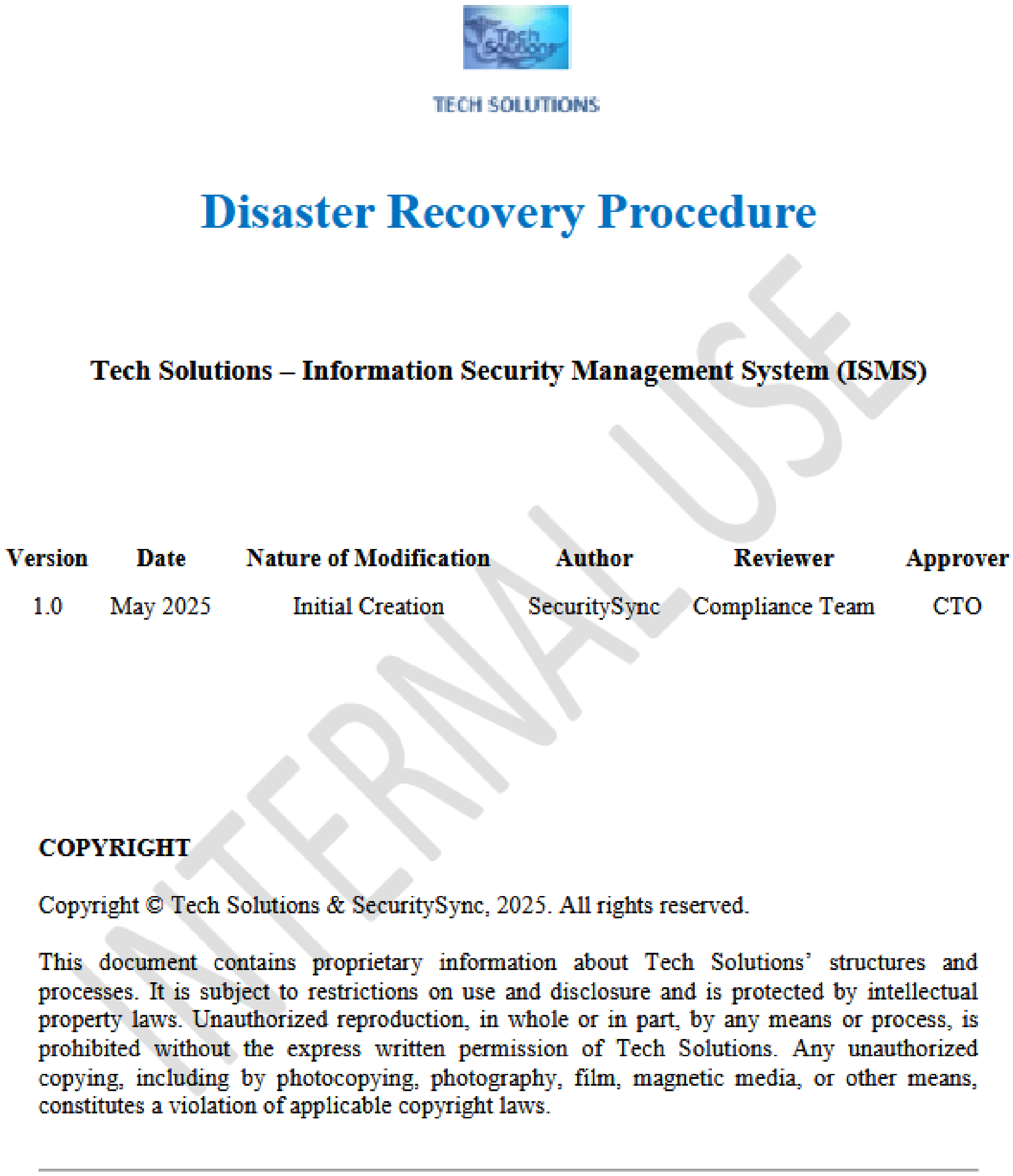
secure. After the test, they find it took too long to restore access, so they update the plan to make it faster)

- Include security tools (like firewalls, antivirus, or encryption) in your business and IT recovery plans. (Example: The business ensures its backup server (used during a disruption) has the same antivirus software and firewall as the main server. They also include a tool to monitor for unauthorized access during the disruption)
- Have ways to keep your normal security measures working, even when things go wrong. (Example: The business normally uses multi-factor authentication (MFA) to protect employee logins. During a power outage, their main office is down, but they ensure employees can still use MFA by setting up a cloud-based authentication system that works remotely)
- If a security measure stops working during a disruption, have a backup plan (a “compensating control”) to protect information. (Example: During a flood, the business’s main office (where they store paper records) is inaccessible, and their normal physical security (locked doors and security cameras) isn’t available. As a compensating control, they temporarily move critical paper records to a secure off-site storage facility with 24/7 security)

Control evidence:

Checks to be performed	Evidence
➢ If a business analysis impact related to information security is carried out ➢ Whether the information security requirements applicable to adverse situations are determined, in light of the results of the business analysis impact ➢ Whether there is an adequate management structure to prepare for, mitigate and respond to a disruptive event ➢ If Business Continuity Plans (BCP) for each critical activity are developed ➢ Whether staff are trained to implement these plans ➢ If these plans are updated regularly ➢ If these plans are tested regularly ➢ Whether test results are analyzed with management and relevant stakeholders	➢ Business impact analysis report ➢ Disaster Recovery Management Structure Designation Note ➢ PCAs and their update dates ➢ PCA test reports ➢ Audit report on the validity and effectiveness of continuity measures

1.2 Practical Application of Clause 5.29: Case Study: ”Tech Solutions”



TECH SOLUTIONS

Disaster Recovery Procedure

Tech Solutions – Information Security Management System (ISMS)

Version	Date	Nature of Modification	Author	Reviewer	Approver
1.0	May 2025	Initial Creation	SecuritySync	Compliance Team	CTO

COPYRIGHT

Document History

Intervenant	Action	Date	Version
Jane Doe, CISO	Creation	05/01/2025	V1.0
John Smith, CTO	Review	05/03/2025	V1.0

1. Introduction

This **Disaster Recovery Policy** outlines the procedures and controls Tech Solutions implements to maintain or restore information security during disruptions, such as cyberattacks, natural disasters, or system failures. The policy applies to all Tech Solutions employees, contractors, and third-party vendors involved in maintaining or restoring critical systems, applications, or data. It addresses the need to protect the confidentiality, integrity, and availability (CIA triad) of information assets during disruptions, ensuring compliance with legal, regulatory, and contractual obligations.

Given the rapid evolution of technology, this policy is a living document, subject to regular updates to reflect changes in systems, risks, or business requirements.

2. Terminology and Normative References

Normative References

This policy is developed in accordance with:

- **ISO 22301:2019** – Business Continuity Management Systems – Requirements
- **ISO 27002:2022** – Information security, cybersecurity, and privacy protection – Information security controls (Clause 5.29)
- **ISO 27001:2022** – Information Security Management Systems – Requirements

Key Terminology

- **Business Continuity Plan (BCP)**: A comprehensive plan to ensure business operations continue during and after a disruption, including both functional and IT components.
- **Disaster Recovery Plan (DRP)**: A subset of the BCP focused on restoring IT systems, applications, and data after a disruption. Also referred to as the Plan de Reprise d'Activité (PRA).
- **Recovery Time Objective (RTO)**: The maximum acceptable downtime for a system or process before it causes significant harm.
- **Recovery Point Objective (RPO)**: The maximum acceptable data loss, measured as the time between the last backup and the point of failure.
- **Business Impact Analysis (BIA)**: An assessment to identify critical processes, their dependencies, and the impact of disruptions.

3. Scope and Objectives

Scope

This policy applies to all critical IT systems, applications, and data managed by Tech Solutions, including cloud-based platforms, customer data, internal systems, and third-party services. It covers disruptions such as cyberattacks (e.g., ransomware), hardware failures, natural disasters (e.g., floods), and power outages.

Objectives

The objectives are to:

1. Determine information security requirements during disruptions.
2. Integrate information security controls into business continuity and IT continuity plans.
3. Maintain existing security controls during disruptions.
4. Implement compensating controls when standard controls are unavailable.
5. Develop, test, review, and evaluate plans to restore information security within required timeframes.

4. Business Impact Analysis (BIA) Summary

The BIA identifies critical business processes, their dependencies, and the impact of disruptions on Tech Solutions' operations. It informs the RTO and RPO values for each critical system or application.

Key Processes and Stakeholders

The following table lists critical processes and their responsible stakeholders, identified through interviews with department heads:

Process	Responsible Stakeholder
Cloud Platform Operations	Sarah Johnson, IT Director
Customer Data Management	Michael Lee, Data Protection Officer (DPO)
Financial Systems Management	Emma Brown, CFO
HR Systems Management	Lisa Patel, HR Manager
Cybersecurity Monitoring	Jane Doe, Chief Information Security Officer (CISO)

RTO and RPO Analysis

The BIA determined the following RTO and RPO values for critical applications, reflecting business needs, legal requirements, and customer expectations:

Application/System	**RTO**	**RPO**
Cloud Platform (SaaS)	4 hours	1 hour
Customer Data Management System	8 hours	2 hours
Financial and Billing Systems	12 hours	4 hours
HR and Payroll Systems	24 hours	12 hours
Email and Collaboration Tools	8 hours	4 hours
Internet Connectivity	4 hours	N/A

Analysis:

- **RTO**: Critical systems like the cloud platform and customer data management require rapid recovery (4-8 hours) due to their direct impact on revenue and customer trust. Less critical systems, like HR, tolerate longer downtimes (24 hours).
- **RPO**: The cloud platform and customer data systems require minimal data loss (1-2 hours) to maintain service integrity. Financial systems can tolerate up to 4 hours of data loss, aligning with daily backup schedules.
- **Communication Needs**: Restoring email and internet connectivity is a priority to support crisis communication and coordination.

5. Information Security Requirements During Disruption

Per **ISO 27002:2022 Clause 5.29**, Tech Solutions has identified the following information security requirements to maintain the CIA triad during disruptions:

1. **Confidentiality**: Prevent unauthorized access to sensitive data (e.g., customer PII, financial records) during recovery operations.
2. **Integrity**: Ensure data accuracy and completeness during restoration, preventing corruption or tampering.
3. **Availability**: Restore critical systems and data within the defined RTO to minimize operational impact.
4. **Compliance**: Adhere to legal and regulatory requirements (e.g., GDPR, CCPA) during disruptions, including data breach notification obligations.
5. **Access Control**: Maintain strict access controls to prevent unauthorized access to systems or data during recovery.

These requirements are embedded in Tech Solutions' **Business Continuity Plan (BCP)** and **Disaster Recovery Plan (DRP)**, ensuring security is not compromised during adverse situations.

6. Disaster Recovery Organization and Responsibilities

Tech Solutions has established a structured crisis management framework to execute the DRP, with clear roles and responsibilities to ensure effective response and recovery.

6.1 Crisis Management Structure

The disaster recovery organization operates at three levels:

1. **Crisis Decision Committee (CDC)**: Makes strategic decisions, such as activating the DRP or escalating to external authorities.
2. **Crisis Operational Committee (COC)**: Coordinates recovery efforts, ensuring alignment with security and business objectives.
3. **Operational Teams**: Execute specific recovery tasks, such as system restoration or data recovery.

6.2 Roles and Responsibilities

Crisis Decision Committee (CDC)

- **Members**:
  - John Smith, CTO (Chair)
  - Jane Doe, CISO (Deputy Chair)
  - Emma Brown, CFO
- **Responsibilities**:
  - Assess the severity and impact of the disruption.
  - Approve activation of the DRP or specific recovery plans.
  - Authorize expenditures for recovery efforts.
  - Coordinate with external stakeholders (e.g., regulators, customers).
  - Ensure compliance with legal and contractual obligations.
  - Oversee crisis communication (internal and external).

Contact Details:

Name	Role	Phone	Email
John Smith	CTO	+1-555-123-4567	john.smith@techsolutions.com
Jane Doe	CISO	+1-555-123-4568	jane.doe@techsolutions.com
Emma Brown	CFO	+1-555-123-4569	emma.brown@techsolutions.com

Crisis Operational Committee (COC)

- **Members**:
  - Sarah Johnson, IT Director (Coordinator)
  - Michael Lee, DPO
  - Lisa Patel, HR Manager
- **Responsibilities**:
  - Implement recovery plans as directed by the CDC.
  - Coordinate operational teams and monitor progress.

  - Ensure information security controls are maintained during recovery.
  - Report recovery status to the CDC.
  - Manage communication with operational teams and third-party vendors.

Contact Details:

Name	Role	Phone	Email
Sarah Johnson	IT Director	+1-555-123-4570	sarah.johnson@techsolutions.com
Michael Lee	DPO	+1-555-123-4571	michael.lee@techsolutions.com
Lisa Patel	HR Manager	+1-555-123-4572	lisa.patel@techsolutions.com

Operational Teams

- **Teams and Responsibilities**:
  - **IT Recovery Team**: Restores servers, networks, and applications (Led by Alex Carter, IT Manager).
  - **Data Recovery Team**: Recovers data from backups and validates integrity (Led by Maria Gomez, Data Engineer).
  - **Security Team**: Monitors for security threats and maintains access controls (Led by Tom Nguyen, Security Analyst).
  - **Logistics Team**: Manages physical resources, such as hardware transport to a recovery site (Led by David Kim, Facilities Manager).
  - **Communication Team**: Handles internal and external communications (Led by Rachel Lee, PR Manager).

Contact Details:

Name	Role	Phone	Email
Alex Carter	IT Manager	+1-555-123-4573	alex.carter@techsolutions.com
Maria Gomez	Data Engineer	+1-555-123-4574	maria.gomez@techsolutions.com
Tom Nguyen	Security Analyst	+1-555-123-4575	tom.nguyen@techsolutions.com
David Kim	Facilities Mgr	+1-555-123-4576	david.kim@techsolutions.com
Rachel Lee	PR Manager	+1-555-123-4577	rachel.lee@techsolutions.com

6.3 External Stakeholders

Key external vendors and partners are included in the recovery process:

- **Cloud Provider**: Restores cloud infrastructure (e.g., AWS, Azure).
- **Internet Service Provider**: Restores connectivity.
- **Security Vendor**: Provides incident response support (e.g., CrowdStrike).
- **Legal Counsel**: Advises on compliance and regulatory obligations.

External Contact Directory:

Entity	Contact Name	Phone	Email
AWS Support	Support Team	+1-800-123-4567	support@aws.com

Verizon ISP	Network Support	+1-800-123-4568	support@verizon.com
CrowdStrike	Incident Team	+1-800-123-4569	incident@crowdstrike.com
Legal Counsel	Anna White	+1-555-123-4580	anna.white@lawfirm.com

7. Information Security Controls in Continuity Plans

Tech Solutions integrates the following information security controls into its BCP and DRP to maintain security during disruptions:

7.1 Security Controls and Tools

- **Access Controls**: Multi-factor authentication (MFA) remains enforced on all recovery systems, with temporary credentials issued for emergency access (e.g., limited-time admin accounts).
- **Encryption**: Data in transit and at rest is encrypted using AES-256, including backups stored off-site or in the cloud.
- **Firewalls and Intrusion Detection**: Network firewalls and intrusion detection systems (IDS) are deployed on recovery servers to prevent unauthorized access.
- **Antivirus and Endpoint Protection**: All recovery endpoints run updated antivirus software to mitigate malware risks.
- **Monitoring Tools**: Security Information and Event Management (SIEM) tools (e.g., Splunk) monitor recovery operations for suspicious activity.
- **Backup Systems**: Regular backups are stored in a secure, off-site location and a cloud repository, with integrity checks performed before restoration.

7.2 Processes to Maintain Existing Controls

Tech Solutions ensures existing security controls remain operational during disruptions through:

- **Cloud-Based Authentication**: MFA is hosted on a cloud platform (e.g., Okta), ensuring availability during on-premises outages.
- **Redundant Network Security**: Backup firewalls and IDS are pre-configured at the recovery site to maintain network protection.
- **Automated Monitoring**: SIEM tools continue logging and alerting, even in degraded modes, to detect threats during recovery.
- **Regular Backup Validation**: Backups are tested monthly to ensure they are secure and restorable, minimizing risks during recovery.

7.3 Compensating Controls

When standard controls cannot be maintained (e.g., due to hardware failure or connectivity loss), the following compensating controls are implemented:

- **Manual Access Verification**: If MFA is unavailable, temporary manual verification (e.g., phone-based approval by the CISO) is used for critical system access.
- **Offline Data Validation**: If automated integrity checks fail, manual data validation is performed by the Data Recovery Team using checksums.

- **Physical Security for Backups**: If cloud backups are inaccessible, physical backups are retrieved from a secure off-site vault with 24/7 guarding.
- **Temporary Firewalls**: Portable firewall appliances are deployed at the recovery site if primary firewalls are down.
- **Incident Response Team**: An external security vendor (e.g., CrowdStrike) is engaged to provide additional monitoring and threat response if internal systems are compromised.

8. Recovery and Restoration Procedures

8.1 Activation Process

The DRP is activated when a disruption exceeds the tolerable downtime (RTO) or data loss (RPO) for critical systems. The process follows:

1. **Detection**: The IT or Security Team identifies the disruption (e.g., ransomware alert from SIEM).
2. **Escalation**: The incident is reported to the COC, which assesses severity and notifies the CDC.
3. **Decision**: The CDC approves DRP activation based on BIA and incident impact.
4. **Communication**: The Communication Team informs stakeholders (employees, customers, regulators) per the crisis communication plan.

8.2 Recovery Workflow

The recovery process is divided into phases:

1. **Initial Response**:
   - Isolate affected systems to prevent further damage (e.g., disconnect compromised servers).
   - Deploy compensating controls (e.g., temporary firewalls).
   - Notify external vendors (e.g., cloud provider, security vendor).
2. **System Restoration**:
   - Restore critical systems from backups (prioritized by RTO).
   - Validate data integrity using checksums or hash verification.
   - Reconfigure network settings and security controls on recovery servers.
3. **Security Validation**:
   - Conduct security scans to ensure no residual threats (e.g., malware scans).
   - Verify access controls and encryption are operational.
   - Test system functionality in a sandbox environment before going live.
4. **Return to Normal Operations**:
   - Gradually migrate operations back to primary systems or confirm recovery site stability.
   - Update incident logs and conduct a post-incident review.

8.3 Crisis Communication Plan

- **Internal Communication**: Employees are informed via email, Slack, or phone trees about the disruption, recovery status, and safety protocols.
- **External Communication**: Customers are notified via email or website updates, with regulatory notifications (e.g., GDPR 72-hour breach reporting) handled by the DPO.
- **Media Handling**: The PR Manager coordinates all media interactions to maintain brand reputation.

9. Testing, Review, and Evaluation

To ensure the DRP's effectiveness, Tech Solutions conducts regular testing, review, and evaluation:

9.1 Testing

- **Frequency**: Semi-annual tabletop exercises and annual full-scale simulations.
- **Scenarios**: Test scenarios include ransomware attacks, data center floods, and power outages.
- **Metrics**: Measure RTO and RPO adherence, system restoration time, and security control effectiveness.
- **Participants**: All crisis management teams, operational teams, and select third-party vendors.

Example Test Plan:

- **Scenario**: Ransomware encrypts the cloud platform.
- **Steps**:
  1. Simulate isolation of affected systems.
  2. Restore from cloud backups within 4 hours (RTO).
  3. Validate data integrity and security controls.
  4. Document lessons learned and update the DRP.

9.2 Review and Evaluation

- **Frequency**: Annual review or after significant incidents/changes (e.g., new systems, regulations).
- **Process**:
  - Analyze test results and incident reports.
  - Identify gaps in security controls or recovery processes.
  - Update the DRP with corrective actions.
- **Approval**: The CDC approves all updates to ensure alignment with business objectives.

9.3 Integration with Business Continuity

The DRP is integrated with Tech Solutions' BCP, ensuring information security is prioritized alongside operational recovery. Regular audits verify that security controls align with **ISO 22301:2019** and **ISO 27001:2022** requirements.

10. Off-Site Recovery Site

To meet high-availability requirements, Tech Solutions maintains a dedicated off-site recovery data center located 50 miles from the primary facility. Key features include:

- **Infrastructure**: Redundant servers, network equipment, and power supplies.
- **Security**: Physical access controls, 24/7 security personnel, and CCTV.
- **Connectivity**: Dedicated high-speed internet and VPN for secure access.
- **Backups**: Daily encrypted backups stored both on-site and in a cloud repository (AWS S3).
- **Testing**: Quarterly connectivity and system tests to ensure readiness.

The off-site facility supports rapid failover for critical systems, achieving the defined RTO and RPO values.

11. Compliance and Legal Considerations

Tech Solutions ensures compliance with:

- **GDPR**: Data breach notifications within 72 hours, if applicable.
- **CCPA**: Consumer data protection during disruptions.
- **ISO 27001:2022**: Alignment with Annex A controls, including A.5.29 and A.5.30.
- **Contractual Obligations**: SLAs with customers guaranteeing uptime and security.

The DPO and legal counsel review recovery operations to ensure compliance, with documentation maintained for audits.

12. Conclusion

This **Disaster Recovery Policy** ensures Tech Solutions maintains robust information security during disruptions. By integrating security controls into business continuity processes, maintaining existing controls, and implementing compensating measures, Tech Solutions protects its critical assets and ensures rapid recovery. Regular testing, review, and updates keep the policy effective, supporting the company's commitment to operational resilience and customer trust.

1.3 ICT readiness for business continuity (5.30)

Control 5.30:

The organization should plan how to maintain information security at an appropriate level during disruption.

Control attributes:

- Control type: When it acts : Corrective
- Information security properties: Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Respond
- Optional capabilities: Which operational area it belongs to : Continuity
- Security domains: Which domain it relates to : Resilience

Control type	**Information security properties**	**Cybersecurity concepts**	**Optional capabilities**	**Security domains**
Corrective	Availability	Respond	Continuity	Resilience

Control description:

- The BIA is a process to figure out which business activities are most important and what happens if they stop. It looks at the impact (how bad it is) and duration (how long it lasts) of a disruption
- What does it do? It identifies:
  - Prioritized activities: The most critical tasks that must keep going.
  - Recovery Time Objective (RTO): How quickly you need to restart an activity or system after a disruption.
  - Resources needed: What you need to keep those activities running (e.g., computers, software, data).
  - Recovery Point Objective (RPO): How much data you can afford to lose (measured in time, e.g., the last 2 hours of data).

Example:

Imagine you run an online store. The BIA might show that your website (a critical activity) must be back online within 4 hours (RTO) after a server crash, or you'll lose customers. It also shows you need the server, payment system, and customer data (resources). The RPO might be 1 hour, meaning you can afford to lose up to 1 hour's worth of recent orders, so you need backups that are updated at least every hour.

- Continuity Strategies: These are plans to keep ICT systems running or recover them quickly during a disruption. Strategies cover what to do before, during, and after a disruption

  Example:

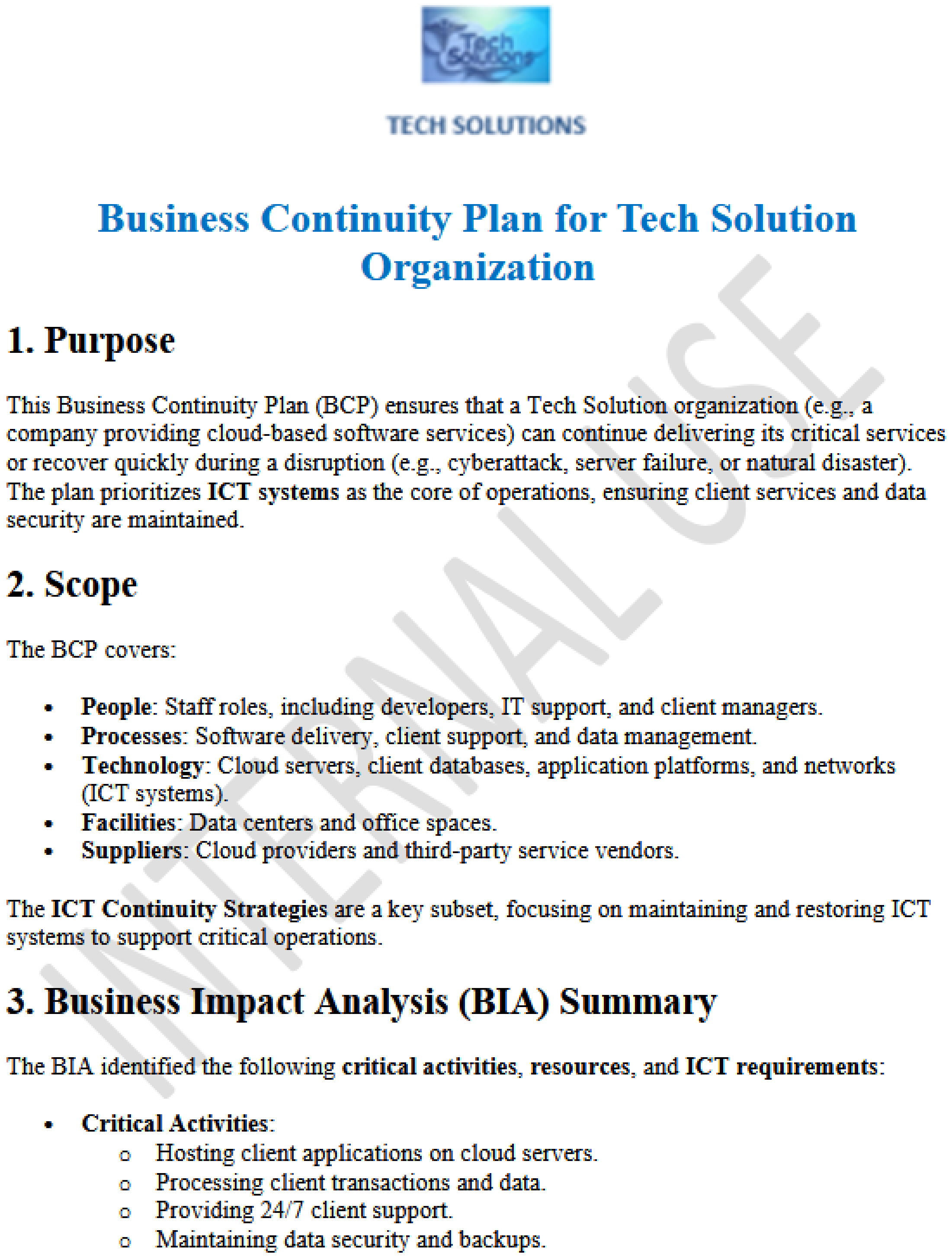
  Your online store might have a strategy to:

  - Before: Store backups of your website data in the cloud.
  - During: Redirect website traffic to a secondary server in another location.
  - After: Restore the main server and sync it with the latest backup.

Control evidence:

Checks to be performed	Evidence
➢ Whether an adequate organizational structure is in place to prepare for, mitigate and respond to a disruption ➢ Whether ICT continuity plans, including response and recovery procedures detailing how the organization plans to manage a disruption to ICT services	➢ ICT continuity plan, ➢ Response and recovery procedures

1.4 Practical Application of Clause 5.30: Case Study: ”Tech Solutions”



TECH SOLUTIONS

Business Continuity Plan for Tech Solution Organization

1. Purpose

This Business Continuity Plan (BCP) ensures that a Tech Solution organization (e.g., a company providing cloud-based software services) can continue delivering its critical services or recover quickly during a disruption (e.g., cyberattack, server failure, or natural disaster). The plan prioritizes **ICT systems** as the core of operations, ensuring client services and data security are maintained.

2. Scope

The BCP covers:

- **People**: Staff roles, including developers, IT support, and client managers.
- **Processes**: Software delivery, client support, and data management.
- **Technology**: Cloud servers, client databases, application platforms, and networks (ICT systems).
- **Facilities**: Data centers and office spaces.
- **Suppliers**: Cloud providers and third-party service vendors.

The **ICT Continuity Strategies** are a key subset, focusing on maintaining and restoring ICT systems to support critical operations.

3. Business Impact Analysis (BIA) Summary

The BIA identified the following **critical activities**, **resources**, and **ICT requirements**:

- **Critical Activities**:
  - Hosting client applications on cloud servers.
  - Processing client transactions and data.
  - Providing 24/7 client support.
  - Maintaining data security and backups.

- **Impact of Disruption**:
  - Loss of revenue if client applications are offline for more than 2 hours.
  - Breach of client trust if data is lost or compromised.
  - Regulatory penalties for failing to meet service-level agreements (SLAs).
- **Recovery Time Objectives (RTO)**:
  - Cloud servers: Restore within **2 hours**.
  - Client database: Restore within **3 hours**.
  - Client support system: Restore within **4 hours**.
- **Recovery Point Objectives (RPO)**:
  - Client database: Maximum data loss of **30 minutes** (backups every 30 minutes).
  - Transaction logs: Maximum data loss of **15 minutes**.
- **ICT Resources Needed**:
  - Cloud server infrastructure.
  - Client database and transaction processing systems.
  - Client support ticketing system.
  - Network and firewall systems.
- **Performance and Capacity**:
  - Cloud servers must support **1,000 concurrent users** during recovery.
  - Transaction system must process **500 transactions per minute**.

4. Organizational Structure

An **Incident Response Team** is established to manage disruptions:

- **Team Leader**: Chief Technology Officer (CTO) with authority to make decisions.
- **IT Operations Lead**: Manages server and database recovery.
- **Security Specialist**: Ensures data integrity and mitigates cyber threats.
- **Client Support Manager**: Handles client communications and support.
- **Training**: Team members receive quarterly training on BCP procedures.
- **Contact List**: Stored in a secure, cloud-based system accessible during disruptions.

5. Business Continuity Strategies

These strategies ensure the organization can continue delivering tech services across all functions:

5.1 People

- **Strategy**: Enable remote work for all staff using secure VPNs and cloud-based collaboration tools (e.g., Microsoft Teams, Slack).
- **Action**: Provide laptops with pre-configured access to critical systems and conduct annual remote work drills.

5.2 Processes

- **Strategy**: Implement manual workarounds for client support and transaction logging if systems are down.
- **Action**: Train client support staff to log tickets offline using secure spreadsheets, syncing data once systems are restored.

5.3 Technology (ICT Continuity Strategies)

The ICT Continuity Strategies are a **subset** of the BCP, focusing on maintaining and restoring ICT systems. They are based on BIA outputs and risk assessments.

5.3.1 Before Disruption

- **Cloud Infrastructure**:
  - Deploy **redundant cloud servers** across multiple geographic regions (e.g., AWS regions in US-East and EU-West).
  - Configure **load balancers** to distribute traffic and ensure high availability.
- **Data Protection**:
  - Schedule **incremental backups** of client databases every 30 minutes and transaction logs every 15 minutes to a secure cloud storage (RPO compliance).
  - Encrypt all backups using AES-256 encryption.
- **Security**:
  - Deploy firewalls and intrusion detection systems to prevent cyberattacks.
  - Conduct monthly vulnerability scans and patch management.
- **Capacity Planning**:
  - Ensure cloud servers are scaled to handle **1,000 concurrent users** and **500 transactions per minute** during recovery.

5.3.2 During Disruption

- **Server Recovery**:
  - Switch to **backup cloud servers** in a secondary region within **2 hours** (RTO) using automated failover scripts.
  - Procedure: IT Operations Lead triggers failover via cloud provider dashboard (e.g., AWS Console).
- **Database Recovery**:
  - Restore client database from the latest backup within **3 hours** (RTO).
  - Procedure: IT Operations Lead retrieves encrypted backup from cloud storage and deploys it to the restored server.
- **Client Support System**:
  - Restore ticketing system within **4 hours** (RTO) using a backup instance.
  - Procedure: Use a pre-configured backup server to host the ticketing system temporarily.
- **Data Integrity**:
  - Verify restored data against transaction logs to ensure no corruption (RPO of 15-30 minutes).
  - Procedure: Security Specialist runs integrity checks using database validation tools.

5.3.3 After Disruption

- **System Restoration**:
  - Revert to primary cloud servers once the issue is resolved (e.g., after patching a vulnerability).
  - Sync restored servers with the latest backup data.
- **Post-Incident Review**:
  - Conduct a root cause analysis within 48 hours to identify and address the disruption's cause.
  - Update BCP and ICT strategies based on lessons learned.

5.4 Facilities

- **Strategy**: Use redundant data centers to ensure server availability.
- **Action**: Contract with multiple cloud providers (e.g., AWS and Azure) to host critical systems in separate data centers.

5.5 Suppliers

- **Strategy**: Maintain contracts with multiple cloud providers to avoid single-point-of-failure risks.
- **Action**: Review SLAs with providers quarterly to ensure they meet RTO and RPO requirements.

6. ICT Continuity Plan Details

The ICT Continuity Plan, as part of the BCP, includes:

- **Performance and Capacity Specifications**:
  - Cloud servers: Support **1,000 concurrent users** and **500 transactions per minute**.
  - Network: Minimum bandwidth of **1 Gbps** to handle client traffic.
- **RTO Procedures**:
  - Cloud servers: Failover to backup region within **2 hours** (automated script execution).
  - Client database: Restore from backup within **3 hours** (manual deployment by IT Operations Lead).
  - Ticketing system: Activate backup instance within **4 hours** (pre-configured server).
- **RPO Procedures**:
  - Client database: Restore data from backups taken every **30 minutes** (cloud storage retrieval).
  - Transaction logs: Recover logs from backups taken every **15 minutes** (validation and sync).

7. Testing and Evaluation

- **Frequency**: Conduct **biannual tests** (every 6 months) to simulate disruptions (e.g., server failure, ransomware attack).
- **Test Scenarios**:
  - Failover to backup cloud servers.
  - Restore client database from backups.
  - Operate client support system offline.
- **Evaluation**:
  - Measure actual recovery times against RTOs (2-4 hours).
  - Verify data loss against RPOs (15-30 minutes).
  - Document test results and update the BCP as needed.
- **Approval**: All tests and plan updates are reviewed and approved by the CTO.

8. Plan Approval

- **Approved by**: Chief Technology Officer (CTO).
- **Date**: May 07, 2025.
- **Review Frequency**: Annually or after major disruptions.

9. Maintenance

- **Updates**: Revise the BCP after tests, incidents, or changes in technology (e.g., new cloud provider).
- **Communication**: Share the plan with all staff via a secure internal portal and provide annual training.

1.5 Legal, statutory, regulatory and contractual requirements (5.31)

Control 5.31:

The organization should plan how to maintain information security at an appropriate level during disruption.

Control attributes:

- Control type: When it acts : Corrective
- Information security properties: Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Identify
- Optional capabilities: Which operational area it belongs to : Legal_and_compliance
- Security domains: Which domain it relates to : Governance_and_Ecosystem, Protection

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Preventive	Confidentiality Integrity Availability	Identify	Legal_and_compliance	Governance_and_Ecosystem Protection

Control description:

- When you create rules or guidelines for protecting information (like a policy saying "all passwords must be strong"), you need to make sure they follow external laws or contracts.

  Example: If your country has a data protection law (like GDPR in Europe) requiring encryption of personal data, your policy must include encryption to comply with that law.

- When you set up tools or processes to protect information (like firewalls or access controls), they must meet legal or contractual requirements.

  Example: If a contract with a client requires two-factor authentication (2FA) for accessing their data, you must implement 2FA to meet that requirement.

- When you label data or equipment (e.g., "confidential" or "public") to decide how to protect it, you need to consider external rules

  Example: A healthcare company must label patient records as "highly confidential" because laws like HIPAA (in the USA) require strict protection of medical data

- When you identify risks to your information (like hacking or data leaks) and decide how to handle them, you must consider external requirements

  Example: If a regulation requires you to report data breaches within 72 hours, your risk plan must include a process to detect and report breaches quickly

- When you decide who is responsible for security tasks (e.g., who monitors for threats), you need to ensure those roles align with external rules

  Example: A law might require a Data Protection Officer (DPO) to oversee personal data. Your company must assign someone to that role

- When you work with suppliers (e.g., cloud storage providers), their contracts must include security requirements that meet external rules

  Example: If you use a cloud provider and a law requires data to stay in your country, the supplier's contract must specify that data won't be stored abroad

- You need to know all the laws and regulations that apply to your business's information security.

  Example: A small e-commerce business must know about:

  - Local data protection laws (e.g., GDPR if in Europe, CCPA if in California).
  - Payment security rules (e.g., PCI DSS for handling credit card data).
  - Industry-specific regulations (e.g., health data laws for a medical app)

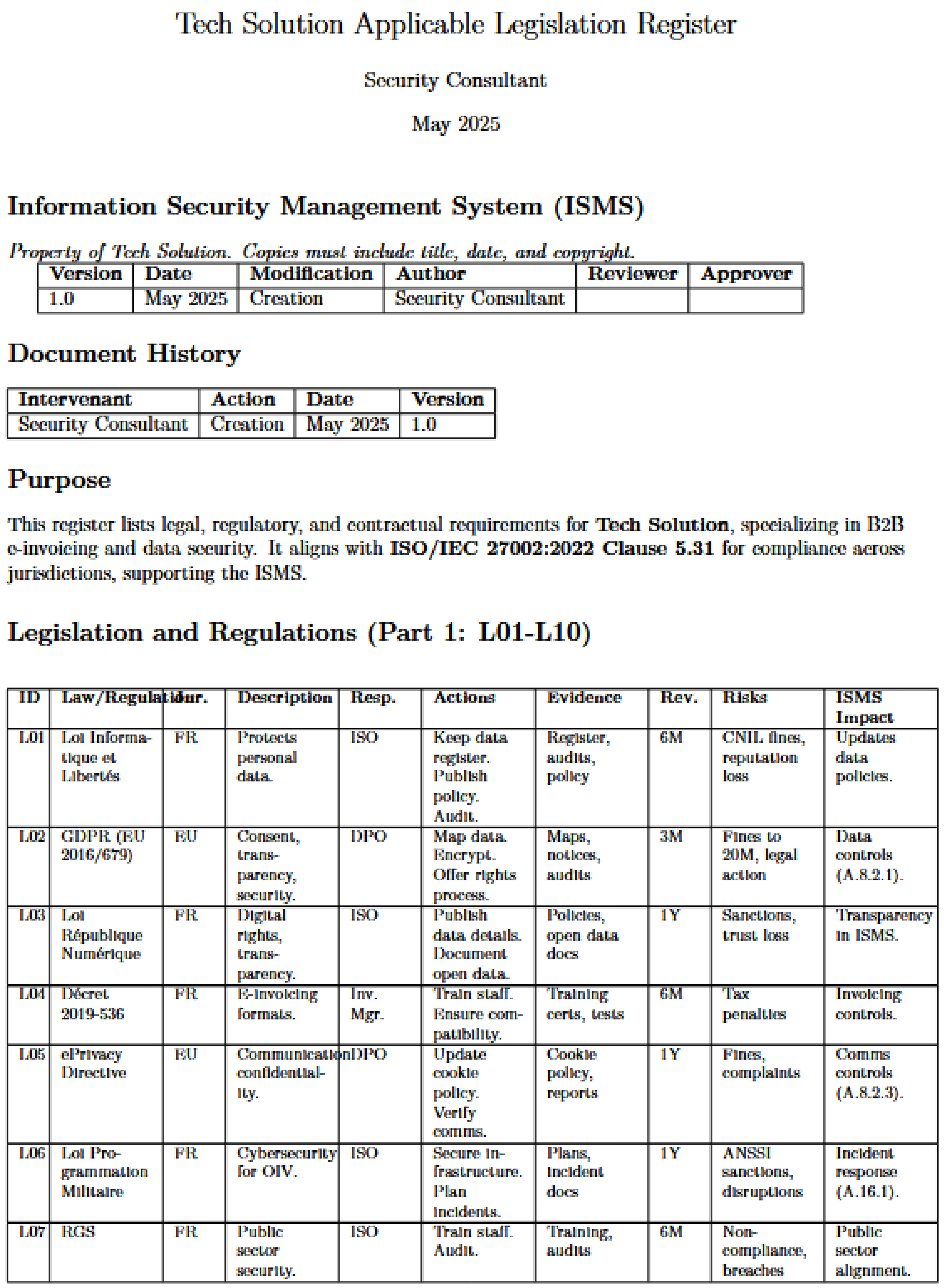
- If your business operates in multiple countries or uses services from other countries, you must follow the laws of those countries too

  Example: If your company is in the USA but uses a cloud provider in Germany, you need to comply with GDPR because the data is processed in Europe

Control evidence:

Checks to be performed	Evidence
➢ Whether external requirements, including legal, statutory, regulatory or contractual requirements, are taken into account ➢ If the organization identifies all relevant legislation and regulations for information security	➢ Documents relating to regulatory, contractual and legal requirements ➢ Document the specific measures and individual responsibilities put in place to meet these requirements

1.6 Practical Application of Clause 5.31: Case Study: ”Tech Solutions”



Tech Solution Applicable Legislation Register

Security Consultant

May 2025

Information Security Management System (ISMS)

Property of Tech Solution. Copies must include title, date, and copyright.

Version	Date	Modification	Author	Reviewer	Approver
1.0	May 2025	Creation	Security Consultant		

Document History

Intervenant	Action	Date	Version
Security Consultant	Creation	May 2025	1.0

Purpose

This register lists legal, regulatory, and contractual requirements for **Tech Solution**, specializing in B2B e-invoicing and data security. It aligns with **ISO/IEC 27002:2022 Clause 5.31** for compliance across jurisdictions, supporting the ISMS.

Legislation and Regulations (Part 1: L01-L10)

ID	Law/Regulation	Jur.	Description	Resp.	Actions	Evidence	Rev.	Risks	ISMS Impact
L01	Loi Informatique et Libertés	FR	Protects personal data.	ISO	Keep data register. Publish policy. Audit.	Register, audits, policy	6M	CNIL fines, reputation loss	Updates data policies.
L02	GDPR (EU 2016/679)	EU	Consent, transparency, security.	DPO	Map data. Encrypt. Offer rights process.	Maps, notices, audits	3M	Fines to 20M, legal action	Data controls (A.8.2.1).
L03	Loi République Numérique	FR	Digital rights, transparency.	ISO	Publish data details. Document open data.	Policies, open data docs	1Y	Sanctions, trust loss	Transparency in ISMS.
L04	Décret 2019-536	FR	E-invoicing formats.	Inv. Mgr.	Train staff. Ensure compatibility.	Training certs, tests	6M	Tax penalties	Invoicing controls.
L05	ePrivacy Directive	EU	Communication confidentiality.	DPO	Update cookie policy. Verify comms.	Cookie policy, reports	1Y	Fines, complaints	Comms controls (A.8.2.3).
L06	Loi Programmation Militaire	FR	Cybersecurity for OIV.	ISO	Secure infrastructure. Plan incidents.	Plans, incident docs	1Y	ANSSI sanctions, disruptions	Incident response (A.16.1).
L07	RGS	FR	Public sector security.	ISO	Train staff. Audit.	Training, audits	6M	Non-compliance, breaches	Public sector alignment.

ID	Law/Regulation	Jur.	Description	Resp.	Actions	Evidence	Rev.	Risks	ISMS Impact
L08	ISO/IEC 27001:2022	Global	ISMS framework.	ISO	Maintain ISMS. Document risks. Train.	Risk reports, training	1Y	Certification loss, gaps	ISMS framework.
L09	Ordonnance 2021-1190	FR	Cybersecurity for services.	ISO	Update contracts. Document ISMS.	Contracts, ISMS reports	1Y	EU sanctions, disruptions	Supplier mgmt (A.15.1).
L10	Article 289 CGI	FR	10-year invoice retention.	Inv. Mgr.	Archive invoices. Track traceability.	Archives, reports	6M	Tax penalties	Archiving (A.12.4.2).

Legislation and Regulations (Part 2: L11-L20)

ID	Law/Regulation	Jur.	Description	Resp.	Actions	Evidence	Rev.	Risks	ISMS Impact
L11	Décret 2022-1299	FR	E-invoicing by 2026.	Inv. Mgr.	Train clients. Update systems.	Training, update logs	3M	Tax penalties	Invoicing workflows.
L12	Norme NF Z42-026	FR	Digitization standards.	Dig. Mgr.	Train staff. Test processes.	Training, tests	1Y	Document rejection	Digitization compliance.
L13	Factur-X Standard	EU	Hybrid invoicing format.	Inv. Mgr.	Integrate Factur-X. Test interop.	Tests, guides	6M	Client non-compliance	System compatibility.
L14	Ordonnance 2019-359	FR	Public sector e-invoicing.	Inv. Mgr.	Verify formats. Train staff.	Certs, compliance reports	1Y	Invoice rejection	Public invoicing.
L15	Article 88, Loi Finances 2020	FR	Progressive e-invoicing.	Inv. Mgr.	Inform clients. Update processes.	Comms, plans	6M	Tax penalties	Client processes.
L16	Code Pénal 323-1 to 323-7	FR	Penalizes system attacks.	ISO	Train staff. Log incidents.	Training, logs	3M	Prosecution, attacks	Awareness (A.7.2.2).
L17	CNIL E-Invoicing	FR	E-invoicing data protection.	ISO	Follow CNIL. Update policies.	Policies, audits	6M	CNIL fines, complaints	E-invoicing data protection.
L18	DORA (EU 2023/2554)	EU	Financial resilience.	ISO	Continuity plans. Test resilience.	Plans, tests	1Y	EU sanctions, disruptions	Resilience (A.17.1).
L19	PCI DSS (v4.0)	Global	Payment card security.	ISO	Implement controls. Assess annually.	Reports, assessments	1Y	Fines, payment loss	Payment security (A.8.2.1).
L20	NIS2 Directive (EU 2022/2555)	EU	Critical service cybersecurity.	ISO	Enhance risks. Report incidents.	Risk reports, incidents	1Y	EU fines, disruptions	Risk mgmt (A.5.1.1).

Notes

- **Jurisdiction**: FR (France), EU, Global, per Clause 5.31.
- **ISMS Impact**: Links to ISO 27002 controls.
- **Review**: 3M (quarterly), 6M (semi-annual), 1Y (annual).
- **Risks**: Financial, legal, operational, reputational.
- **Evidence**: Reports, logs, training.

Tech Solution reviews this register regularly and consults legal experts for international requirements.

1.7 Intellectual property rights (5.32)

Control 5.32:

The organization should implement appropriate procedures to protect intellectual property rights.

Control attributes:

- Control type: When it acts : Corrective
- Information security properties: Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Identify
- Optional capabilities: Which operational area it belongs to : Legal_and_compliance
- Security domains: Which domain it relates to : Governance_and_Ecosystem,

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Preventive	Confidentiality Integrity Availability	Identify	Legal_and_compliance	Governance_and_Ecosystem

Control description:

- Create a clear rule (policy) that explains how your organization protects IP, like software, documents, or designs. Share this policy with everyone in the company.

  Example: Your company writes a policy saying, "All employees must use only licensed software and not copy or share company designs without permission." This policy is shared during onboarding and posted on the company's internal website.

- Write step-by-step instructions on how to use software, documents, or other IP legally (e.g., how to install software or share files).

  Example: Your IT team creates a guide that says, “To install Adobe Photoshop, get approval from the IT manager and use the official license key provided by the company. Do not download it from random websites.”

- Buy or download software only from trusted places (like the official website or authorized vendors) to avoid pirated or illegal versions.

  Example: Instead of downloading Microsoft Office from a shady website, your company purchases it directly from Microsoft’s website or an authorized retailer like Amazon Business.

- Keep a list (register) of all IP assets (like software, patents, or designs) and note which ones need special protection.

  Example: Your company maintains a spreadsheet listing all software (e.g., “Adobe Illustrator, License #12345, used by Design Team”) and marks which ones have copyright or licensing rules.

- Keep records (like receipts, license certificates, or manuals) to prove your company legally owns the IP it uses.

  Example: Your IT department saves the purchase receipt and license key for Zoom in a folder, so if someone asks, you can prove it was bought legally.

- Make sure only the allowed number of people or devices use a licensed product, as stated in the license agreement.

  Example: Your company buys a license for 10 users of a project management tool. You ensure only 10 employees use it and don’t share the login with others.

- Regularly check computers and devices to confirm that only legal, approved software is installed.

  Example: Every six months, the IT team scans all company laptops to check that no one has installed pirated software or unapproved apps.

- Have rules for keeping licenses valid, like renewing them on time or following usage terms.

  Example: Your company sets a reminder to renew its antivirus software license every year and assigns an employee to check that the license terms (e.g., “for 50 devices only”) are followed.

- Create rules for what to do when you stop using software or give it to someone else, ensuring you follow legal terms.

Example: If your company stops using a graphic design tool, the IT team deletes it from all computers and checks the license agreement to see if it can be transferred to another company.

- Follow the rules for software or content downloaded from the internet or external sources.

  Example: If you download a free stock photo from a website, you read the terms to ensure it's okay to use in your company's marketing materials without breaking copyright rules

- Don't copy or change commercial videos, music, or other recordings unless the license or law allows it.

  Example: Your company buys a music track for a promotional video. The license says "no remixing." So, you use the track as-is and don't edit or copy it for other uses.

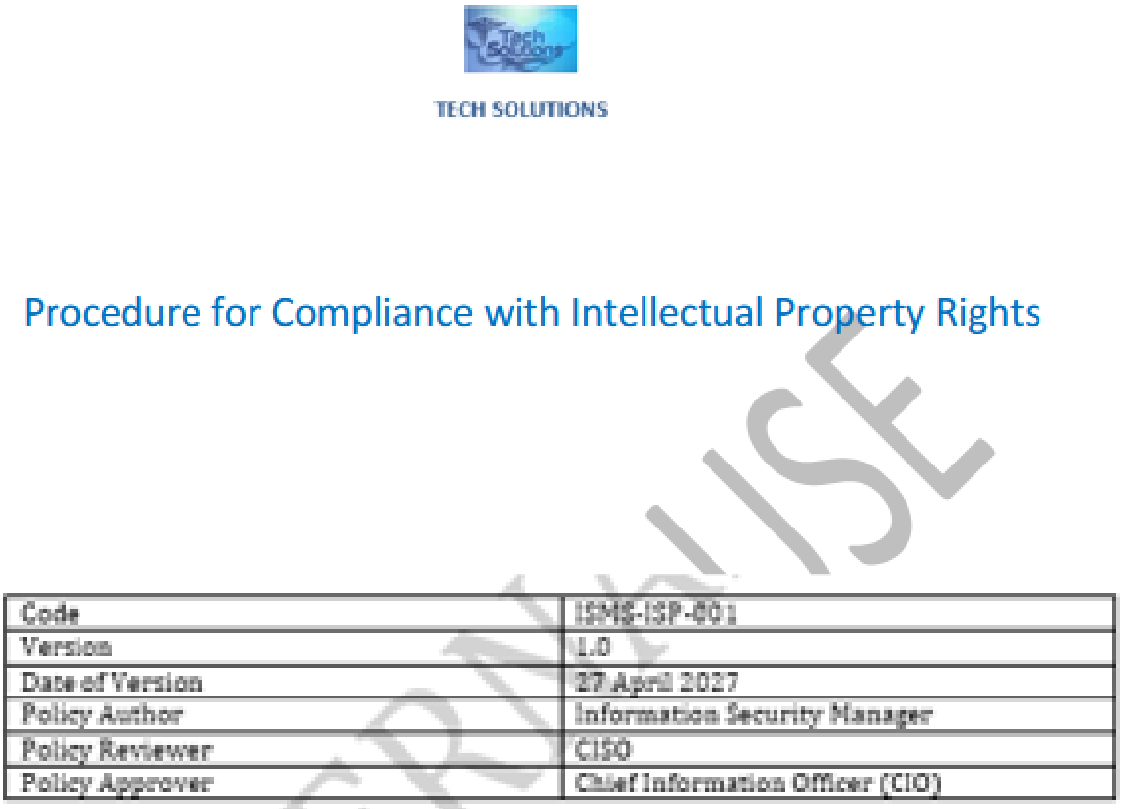
- Don't photocopy or share protected documents (like ISO standards or books) unless the copyright law or license allows it.

  Example: Your company buys a digital copy of an ISO standard. The license says "no sharing." So, you don't email it to others or print extra copies beyond what's allowed.

Control evidence:

Checks to be performed	Evidence
➢ Whether a procedure is developed and implemented to ensure compliance with legal, regulatory and contractual requirements relating to intellectual property and the use of proprietary software licenses ➢ If an inventory of software officially installed and declared on each computer equipment (servers, workstations, network and security equipment, etc.) is kept up to date at all times ➢ If frequent checks are carried out to verify that the installed software complies with the declared software or that it has a valid license ➢ If controls are implemented to ensure that the maximum number of users authorized by the license is not exceeded	➢ Procedure for verifying compliance with legal, regulatory and contractual requirements relating to intellectual property and the use of proprietary software licenses ➢ Inventory of software officially installed and declared on each computer device ➢ Sample software licenses.

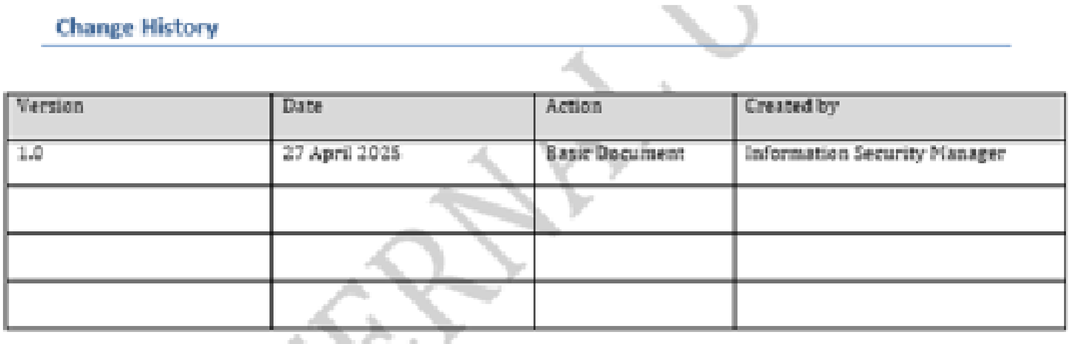
1.8 Practical Application of Clause 5.32: Case Study: ”Tech Solutions”



TECH SOLUTIONS

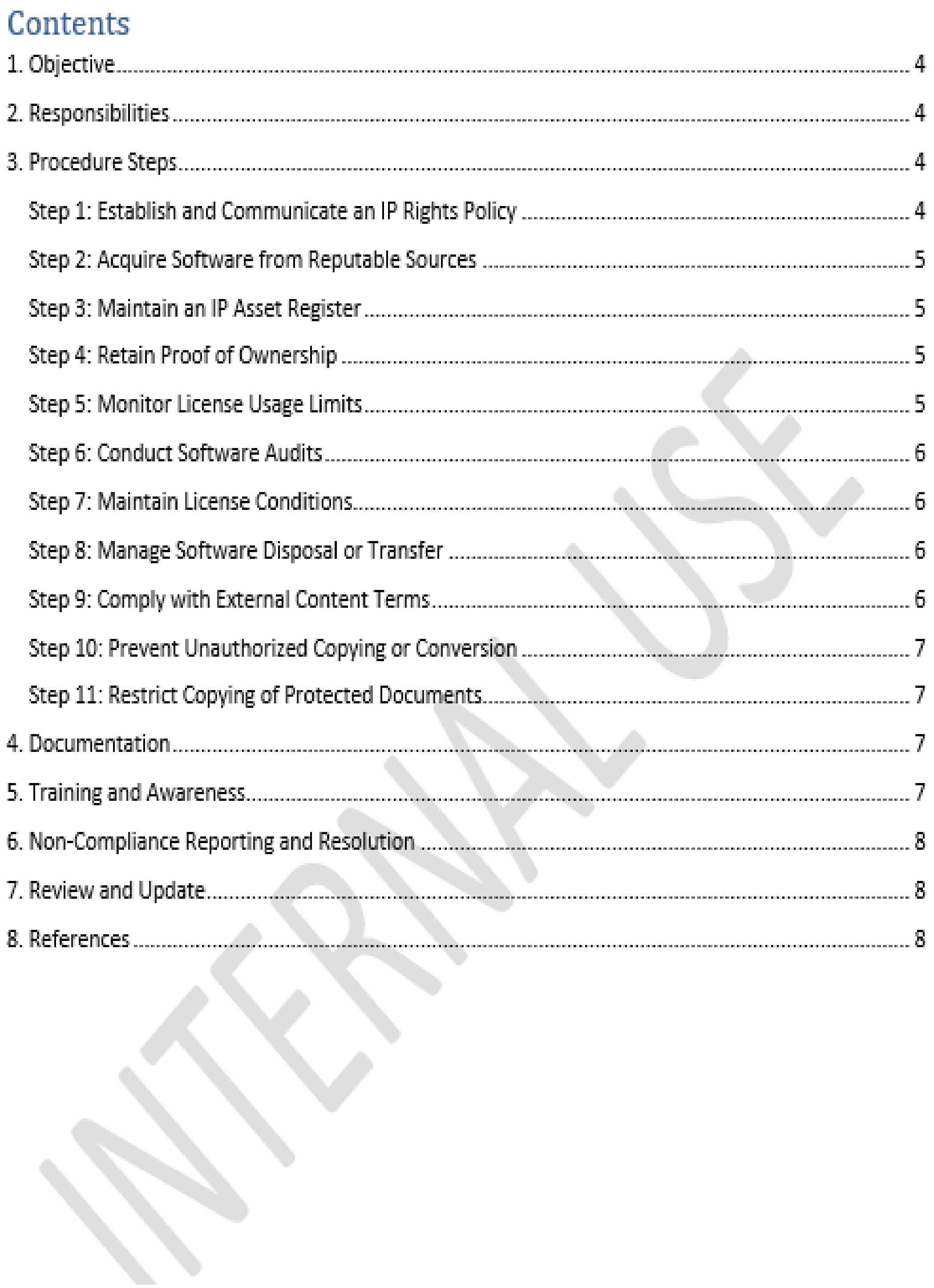
Procedure for Compliance with Intellectual Property Rights

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

Purpose: To ensure Tech Solutions complies with intellectual property rights (IPR) and adhering to legal, regulatory, and contractual requirements for IP and proprietary software licenses.
Scope: Applies to all employees, contractors, and systems using IP or proprietary software at Tech Solutions.

1. Objective

To implement controls to ensure Tech Solutions:

- Respects and protects intellectual property (IP), including software, documents, designs, music, videos, and other copyrighted materials.
- Complies with legal, regulatory, and contractual obligations related to IP rights.
- Prevents unauthorized use, copying, or distribution of IP assets.

2. Responsibilities

- **IT Department**: Manages software licenses, conducts audits, and maintains IP asset registers.
- **Compliance Officer**: Oversees IP policy enforcement and ensures legal compliance.
- **Employees**: Adhere to IP policies and report non-compliance.
- **Management**: Approves software purchases and allocates resources for IP compliance.

3. Procedure Steps

Step 1: Establish and Communicate an IP Rights Policy

- **Objective**: Define and communicate a topic-specific policy on protecting IP rights
- **Action**:
  - The Compliance Officer develops and maintains the "Tech Solutions Intellectual Property Rights Policy," outlining rules for legal use of software, content, and other IP.
  - Distribute the policy via email, the company intranet, and during employee onboarding.
  - Conduct annual training to ensure employees understand the policy.
- **Example**: The policy states, "Employees must use only licensed software from approved vendors and not share copyrighted designs without permission."

Step 2: Acquire Software from Reputable Sources

- **Objective**: Ensure software is acquired only through known and reputable sources to avoid copyright infringement
- **Action**:
  - The IT Department maintains a list of approved vendors (e.g., Microsoft, Adobe, Amazon Business).
  - Before purchasing, verify the vendor's authenticity (e.g., check official websites or contact vendor support).
- **Example**: Tech Solutions purchases Zoom licenses directly from zoom.us, not from third-party discount sites.

Step 3: Maintain an IP Asset Register

- **Objective**: Maintain appropriate asset registers identifying all assets with IP protection requirements
- **Action**:
  - The IT Department uses a software tool (e.g., "AssetTrack") or spreadsheet to list all IP assets (e.g., software, designs, documents).
  - Include details like license number, expiration date, and usage restrictions.
  - Update the register quarterly or when new assets are acquired.
- **Example**: The register lists "Adobe Photoshop, License #45678, Design Team, 5 users, expires 12/31/2025."

Step 4: Retain Proof of Ownership

- **Objective**: Maintain proof and evidence of ownership for licenses, manuals, etc.
- **Action**:
  - Store digital copies of purchase receipts, license keys, and agreements in a secure folder (e.g., "License_Records" on the company server).
  - Keep physical manuals or certificates in a locked cabinet.
- **Example**: The receipt for 50 Microsoft Office licenses is saved as "Office_Receipt_2025.pdf" in the License_Records folder.

Step 5: Monitor License Usage Limits

- **Objective**: Ensure the maximum number of users or resources permitted within the license is not exceeded
- **Action**:
  - Use license management tools (e.g., Microsoft Admin Portal) to track usage.
  - Conduct monthly checks to verify compliance with license terms.
- **Example**: For a 20-user CRM license, IT ensures only 20 accounts are active and desactivates excess accounts.

Step 6: Conduct Software Audits

- **Objective**: Carry out reviews to ensure only authorized software and licensed products are installed
- **Action**:
    - Every six months, the IT Department scans all devices using audit software (e.g., "LanSweeper").
    - Compare installed software against the asset register and remove unauthorized software.
    - Document audit findings in a report.
- **Example**: An audit identifies a pirated video editing tool on an employee's laptop. IT removes it and retrains the employee.

Step 7: Maintain License Conditions

- **Objective**: Provide procedures for maintaining appropriate license conditions
- **Action**:
    - Set reminders for license renewals (e.g., using a calendar or software tool).
    - Assign an IT staff member to monitor compliance with license terms (e.g., user limits, geographic restrictions).
- **Example**: IT sets a reminder to renew antivirus software licenses annually and verifies it covers 100 devices as licensed.

Step 8: Manage Software Disposal or Transfer

- **Objective**: Provide procedures for disposing of or transferring software to others
- **Action**:
    - Check license agreements for disposal or transfer rules (e.g., "non-transferable" or "requires vendor approval").
    - Delete software from devices before disposal and document the process.
- **Example**: When discontinuing an accounting tool, IT deletes it from all systems and records "Software X removed on 5/1/2025" in the asset register.

Step 9: Comply with External Content Terms

- **Objective**: Comply with terms and conditions for software and information from public networks or external sources
- **Action**:
    - Train employees to review terms of use for downloaded content (e.g., stock photos, open-source software).
    - Document compliance checks for external content.
- **Example**: An employee downloads a free stock image and confirms it's licensed for commercial use before including it in a marketing campaign.

Step 10: Prevent Unauthorized Copying or Conversion

- **Objective**: Prohibit duplicating, converting, or extracting from commercial recordings unless permitted
- **Action**:
  - Include rules in the IP policy (e.g., "Do not copy or remix commercial music or videos without permission").
  - Use digital rights management (DRM) tools to restrict copying where applicable.
- **Example**: A marketing team uses a licensed music track for a video as-is, without remixing, per the license terms.

Step 11: Restrict Copying of Protected Documents

- **Objective**: Prohibit copying standards, books, articles, reports, or other documents unless permitted
- **Action**:
  - Include rules in the IP policy (e.g., "Do not photocopy or share ISO standards without authorization").
  - Train employees on copyright limits for documents.
- **Example**: An employee requests permission from the Compliance Officer before sharing a digital ISO standard with a colleague.

---

4. Documentation

- Maintain records of:
  - IP asset registers (updated quarterly).
  - Audit reports (every six months).
  - License proofs (stored indefinitely).
  - Non-compliance incidents and corrective actions.
- Store records in a secure, access-controlled system (e.g., company server with role-based access).

---

5. Training and Awareness

- Conduct annual training on the IP Rights Policy and this procedure.
- Use real-world examples (e.g., "Using pirated software can lead to fines or lawsuits").
- Provide refresher training after non-compliance incidents.

---

6. Non-Compliance Reporting and Resolution

- Encourage reporting of IP violations via an anonymous channel (e.g., email to compliance@techsolutions.com).
- Investigate reports, take corrective action (e.g., remove unauthorized software, retrain employees), and document outcomes.
- Example: A reported pirated software installation is removed, and the employee attends compliance training.

7. Review and Update

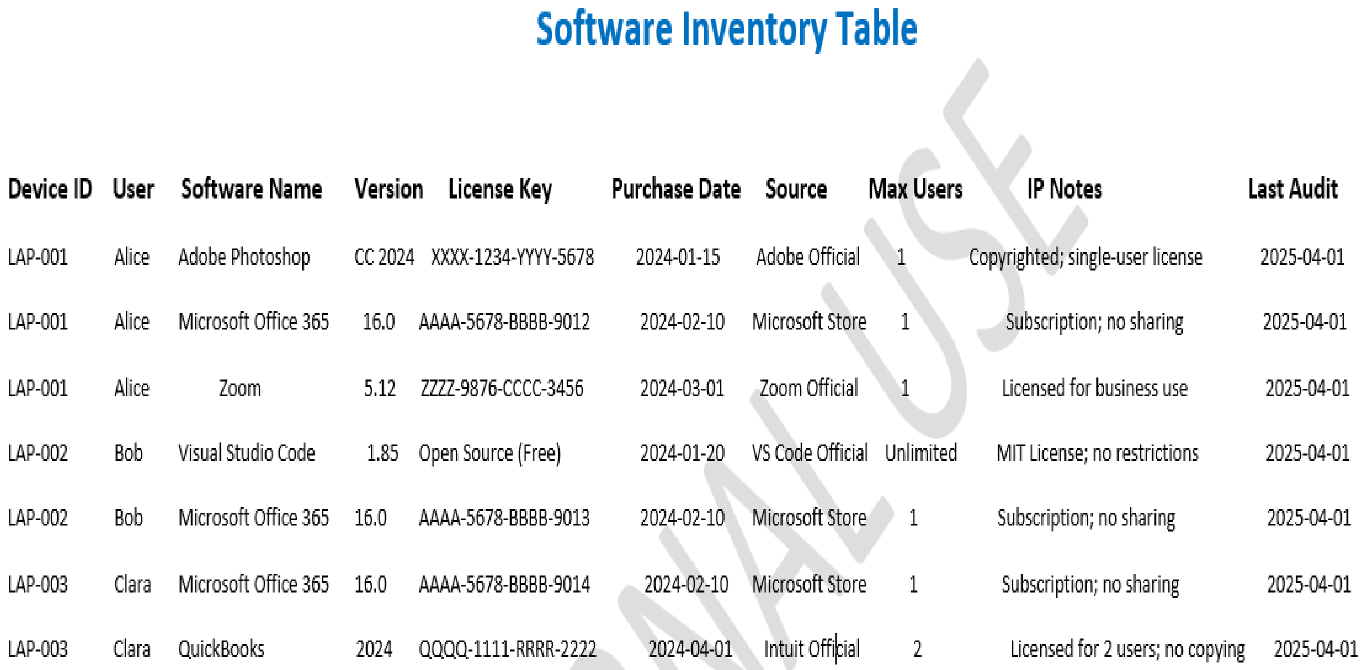
- Review this procedure annually or when laws, regulations, or contracts change.
- The Compliance Officer and IT Department ensure updates align with ISO 27002:2022 and legal requirements.

8. References

- ISO/IEC 27002:2022, Clause 5.32 – Intellectual Property Rights.
- Tech Solutions Intellectual Property Rights Policy (available on intranet).
- Applicable copyright laws and software license agreements.

Approval:

- **Prepared by**: Compliance Officer, Tech Solutions
- **Approved by**: CEO, Tech Solutions
- **Effective Date**: May 15, 2025



Software Inventory Table

Device ID	User	Software Name	Version	License Key	Purchase Date	Source	Max Users	IP Notes	Last Audit
LAP-001	Alice	Adobe Photoshop	CC 2024	XXXX-1234-YYYY-5678	2024-01-15	Adobe Official	1	Copyrighted; single-user license	2025-04-01
LAP-001	Alice	Microsoft Office 365	16.0	AAAA-5678-BBBB-9012	2024-02-10	Microsoft Store	1	Subscription; no sharing	2025-04-01
LAP-001	Alice	Zoom	5.12	ZZZZ-9876-CCCC-3456	2024-03-01	Zoom Official	1	Licensed for business use	2025-04-01
LAP-002	Bob	Visual Studio Code	1.85	Open Source (Free)	2024-01-20	VS Code Official	Unlimited	MIT License; no restrictions	2025-04-01
LAP-002	Bob	Microsoft Office 365	16.0	AAAA-5678-BBBB-9013	2024-02-10	Microsoft Store	1	Subscription; no sharing	2025-04-01
LAP-003	Clara	Microsoft Office 365	16.0	AAAA-5678-BBBB-9014	2024-02-10	Microsoft Store	1	Subscription; no sharing	2025-04-01
LAP-003	Clara	QuickBooks	2024	QQQQ-1111-RRRR-2222	2024-04-01	Intuit Official	2	Licensed for 2 users; no copying	2025-04-01

1.9 Protection of records (5.33)

Control 5.33:

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

Control attributes:

- Control type: When it acts : Corrective
- Information security properties: Availability
- Cybersecurity concepts: Which phase of cybersecurity it supports : Identify, Protect
- Optional capabilities: Which operational area it belongs to : Legal_and_compliance, Asset_management, Information_protection
- Security domains: Which domain it relates to : Defence

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Preventive	Confidentiality Integrity Availability	Identify Protect	Legal_and_compliance, Asset_management, Information_protection	Defence

Control description:

- Create clear rules on how to store, handle, track, and destroy records. These rules should prevent anyone from tampering with records and align with the organization’s records management policy.

Example: Imagine a hospital has patient records. The hospital creates a guideline saying:

Store patient files in a secure, locked cabinet or encrypted digital folder.

Only authorized staff can access them.

Track who accesses the records (chain of custody) to ensure no unauthorized changes.

Destroy old records securely (e.g., shred paper files or wipe digital files) to prevent misuse.

- Decide which records to keep, how long to keep them, and when to destroy them. This schedule should follow laws, regulations, or societal expectations

  Example: A small business keeps:

  Tax records for 7 years (as required by tax laws).

  Employee contracts for 3 years after an employee leaves.

  Customer complaints for 1 year. After these periods, the business can destroy the records if they're no longer needed.

- Group records into types (e.g., financial, legal, personnel) and assign them a security classification (e.g., confidential, public). Specify how long to keep each type and what storage media (paper or digital) to use.

  Example: A school might categorize records like:

  Student grades: Confidential, keep for 5 years, store digitally with encryption.

  Staff payroll: Confidential, keep for 7 years, store in a secure cloud system.

  Public flyers: Non-confidential, keep for 1 year, store on a shared drive.

- Use storage systems (like cloud servers, filing cabinets, or databases) that let you retrieve records quickly and in a usable format.

  Example: A law firm stores client contracts in a cloud system that:

  Allows quick searches by client name or date.

  Keeps files in a format (e.g., PDF) that's easy to open.

  Has backups to prevent data loss.

- If records are stored digitally, ensure they can still be accessed years later, even if technology changes. This includes keeping any encryption keys or software needed to open the files.

  Example: A company stores encrypted financial records from 2015. To access them in 2025:

  They keep the encryption key in a secure vault.

  They ensure the file format (e.g., an old version of Excel) can still be opened by updating software or converting files.

- Use storage devices (like hard drives, USBs, or paper) as recommended by their makers to prevent damage. Also, consider that storage media can degrade over time.

  Example: A museum storing historical records on DVDs follows the manufacturer’s advice:

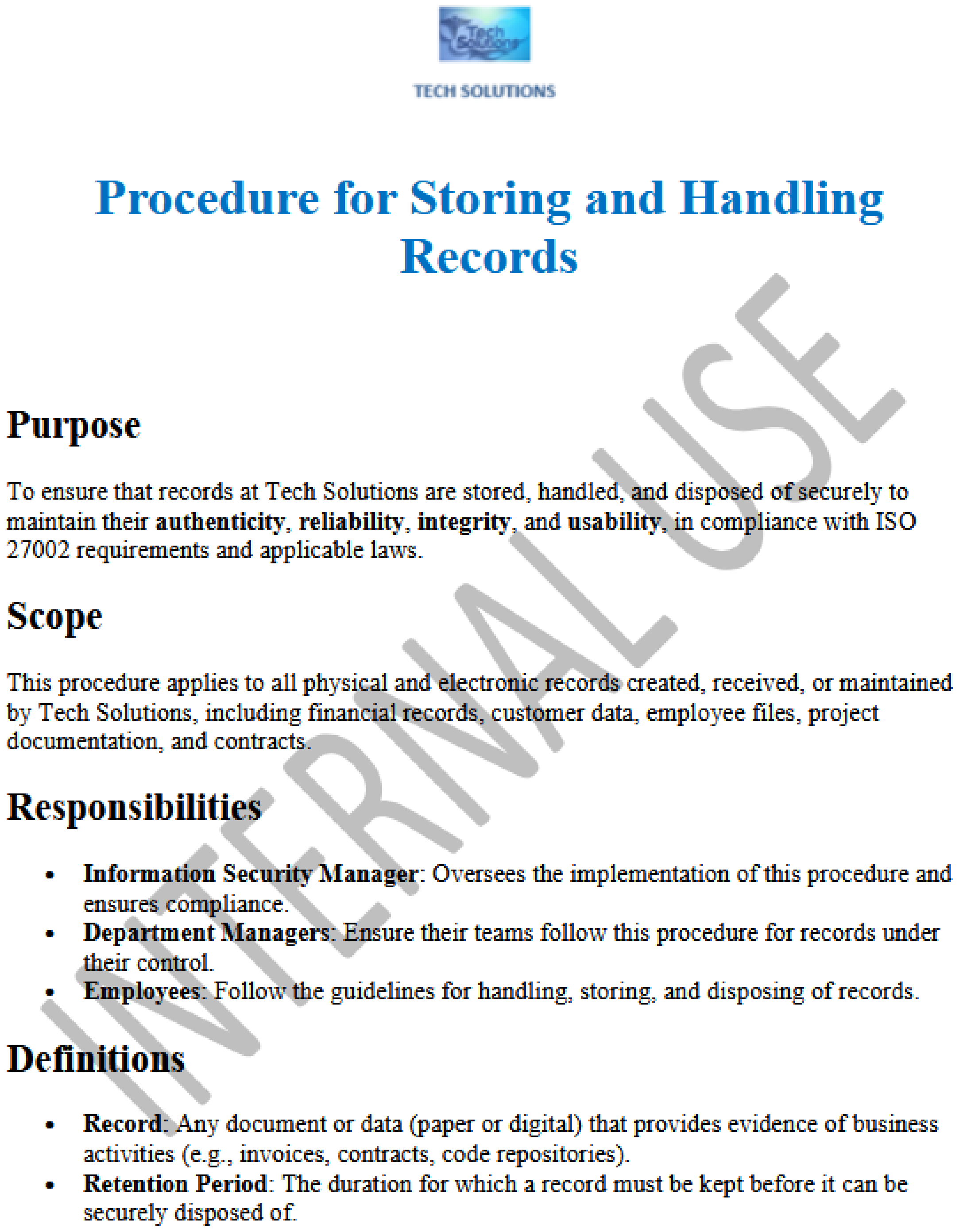
  Keep DVDs in a cool, dry place to avoid damage.

  Check DVDs every few years for signs of deterioration and copy data to new media if needed.

Control evidence:

Checks to be performed	Evidence
➢ If a procedure for storing and handling records is developed and implemented ➢ If recording protection measures are put in place in accordance with their classification	➢ Procedure for storing and handling records

1.10 Practical Application of Clause 5.33: Case Study: ”Tech Solutions”



TECH SOLUTIONS

Procedure for Storing and Handling Records

Purpose

To ensure that records at Tech Solutions are stored, handled, and disposed of securely to maintain their **authenticity**, **reliability**, **integrity**, and **usability**, in compliance with ISO 27002 requirements and applicable laws.

Scope

This procedure applies to all physical and electronic records created, received, or maintained by Tech Solutions, including financial records, customer data, employee files, project documentation, and contracts.

Responsibilities

- **Information Security Manager**: Oversees the implementation of this procedure and ensures compliance.
- **Department Managers**: Ensure their teams follow this procedure for records under their control.
- **Employees**: Follow the guidelines for handling, storing, and disposing of records.

Definitions

- **Record**: Any document or data (paper or digital) that provides evidence of business activities (e.g., invoices, contracts, code repositories).
- **Retention Period**: The duration for which a record must be kept before it can be securely disposed of.

Procedure

1. Guidelines for Storage, Handling, and Disposal

Tech Solutions maintains the following guidelines to protect records:

- **Storage**:
  - **Physical records** (e.g., signed contracts) must be stored in locked filing cabinets in a secure office area with restricted access.
  - **Electronic records** (e.g., customer data, project files) must be stored in the company's encrypted cloud platform (e.g., Microsoft OneDrive with AES-256 encryption).
  - Access to records is restricted to authorized personnel based on their role.
- **Handling and Chain of Custody**:
  - Only authorized employees can access or modify records.
  - All access to sensitive records (e.g., financial or customer data) is logged in the company's document management system.
  - Employees must use secure channels (e.g., encrypted email or secure file transfer) when sharing records internally or externally.
  - Physical records must not be left unattended on desks or in public areas.
- **Disposal**:
  - **Physical records**: Shred using a cross-cut shredder when no longer needed (after the retention period).
  - **Electronic records**: Permanently delete using secure deletion software (e.g., Eraser) to prevent recovery.
  - Disposal must be documented, including the date and method, to maintain an audit trail.
- **Prevention of Manipulation**:
  - Use version control for electronic records (e.g., Git for code, version tracking in document management systems).
  - Apply digital signatures or checksums to critical records to detect unauthorized changes.
- **Alignment with Policy**: These guidelines align with Tech Solutions' **Records Management Policy** and comply with GDPR and local data protection laws.

2. Retention Schedule

Tech Solutions maintains a retention schedule for all records, based on their type, legal requirements, and business needs. Below is an example:

Record Type	Retention Period	Storage Media	Security Classification
Financial Records (e.g., invoices, tax documents)	7 years	Electronic (cloud)	Confidential
Employee Records (e.g., contracts, payroll)	3 years after employment ends	Electronic and Physical	Confidential
Customer Data (e.g., project specifications)	5 years	Electronic (cloud)	Confidential
Contracts with Clients/Suppliers	6 years after contract ends	Electronic and Physical	Confidential
Marketing Materials (e.g., brochures)	1 year	Electronic	Public
Software Code Repositories	Indefinite (business-critical)	Electronic (GitHub)	Restricted

- **Legal Compliance**: Retention periods comply with GDPR, local tax laws, and industry standards.
- **Destruction**: After the retention period, records are securely destroyed unless required for ongoing business or legal purposes.

3. Classification and Categorization

- Records are categorized into types (e.g., financial, employee, customer, legal) and assigned a security classification based on Tech Solutions' **Information Classification Policy**:
  - **Public**: Information available to anyone (e.g., marketing flyers).
  - **Restricted**: Limited to specific teams (e.g., software code).
  - **Confidential**: Highly sensitive (e.g., customer data, financial records).
- Each record type is documented with:
  - Retention period.
  - Approved storage media (physical or electronic).
  - Access controls.

4. Storage Systems

- **Physical Storage**:
  - Locked filing cabinets in a secure office area.
  - Fireproof and waterproof storage for critical records (e.g., original contracts).
- **Electronic Storage**:
  - Use Microsoft OneDrive for cloud storage with encryption and multi-factor authentication (MFA).
  - Ensure records are backed up daily to a secondary encrypted cloud server.

    - Retrieval time: Records must be accessible within 1 hour for urgent requests (e.g., during audits).
- **Format**: Store records in widely compatible formats (e.g., PDF for documents, SQL databases for customer data) to ensure usability.

5. Long-Term Access to Electronic Records

- **Technology Compatibility**:
    - Regularly review file formats to ensure they remain readable (e.g., convert old .doc files to .docx or PDF).
    - Maintain documentation of software versions used for records (e.g., database schemas).
- **Encryption Keys**:
    - Store cryptographic keys for encrypted records in a secure key management system (e.g., Azure Key Vault).
    - Retain keys for the entire retention period of the records.
- **Periodic Checks**:
    - Every 2 years, test a sample of archived records to ensure they can be accessed and are not corrupted.
    - Migrate records to new storage media if the current media risks obsolescence (e.g., from old hard drives to cloud).

6. Storage Media Care

- **Physical Media**:
    - Store paper records in a climate-controlled environment (e.g., 20-22°C, 40-50% humidity) to prevent deterioration.
    - Follow manufacturer guidelines for archival-quality folders and boxes.
- **Electronic Media**:
    - Use enterprise-grade cloud storage (e.g., Microsoft OneDrive) to minimize risks of hardware failure.
    - Check cloud provider’s compliance with ISO 27001 for secure storage.
    - Replace external drives or USBs every 5 years to avoid data loss due to media degradation.

Training and Awareness

- All employees receive annual training on this procedure, including:
    - How to classify and store records.
    - Secure handling and disposal practices.
    - Recognizing and reporting potential record tampering.
- New hires are trained during onboarding.

Monitoring and Review

- The Information Security Manager conducts quarterly audits to ensure compliance with this procedure.
- The retention schedule and storage systems are reviewed annually or when legal/business requirements change.
- Any incidents (e.g., unauthorized access or record loss) must be reported immediately and investigated.

References

- ISO 27002:2022, Section on Records Management.
- Tech Solutions' Records Management Policy.
- GDPR and local data protection regulations.

Approval

- **Prepared by**: Information Security Manager
- **Approved by**: Chief Operating Officer
- **Effective Date**: May 15, 2025

1.11 Privacy and protection of PII (5.34)

Control 5.34:

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

Control attributes:

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

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Preventive	Confidentiality Integrity Availability	Identify Protect	Information_protection Legal_and_compliance	Protection

Control description:

- The organization needs a written policy that explains how it will protect people's personal information (PII). This policy must be shared with everyone who needs to know, like employees, contractors, or partners.

  Example: Imagine you run a small online store. Your privacy policy might say, "We collect customers' names and addresses only to ship products, and we won't share this info with anyone else unless required by law." You share this policy on your website and with your staff so they know the rules.

- You need step-by-step instructions (procedures) on how to handle PII safely. These procedures should be shared with everyone who deals with PII, like employees or third-party vendors.

Example: For your online store, a procedure might be: “When a customer places an order, save their address in a secure database, use encryption to protect it, and delete it after 6 months.” You train your employees and your website developer to follow this procedure.

- The organization must make sure everyone follows the procedures and any privacy laws (like GDPR in Europe or CCPA in California). This involves setting up roles, responsibilities, and controls to keep PII safe.

  Example: In your store, you make sure your staff knows they can’t email customer details to their personal accounts because it violates privacy laws. You also set up a password-protected system to store customer data securely (a control).

- It’s a good idea to have one person (like a privacy officer) responsible for making sure PII is protected. This person guides employees and vendors on what to do and ensures the rules are followed.

  Example: In your store, you assign your trusted manager, Sarah, as the “privacy officer.” Sarah checks that customer data is stored securely, trains new employees on the privacy rules, and answers questions about handling PII.

- When handling PII, the organization must follow the privacy laws that apply to its location or customers. This might mean different rules depending on where the data comes from.

  Example: If your store ships to Europe, Sarah learns about GDPR, which requires getting customer consent before collecting their data. She updates your website to include a “consent checkbox” for customers to agree to share their info

- Use technology (like encryption) and organizational practices (like training or access controls) to protect PII from being stolen, lost, or misused.

  Example:

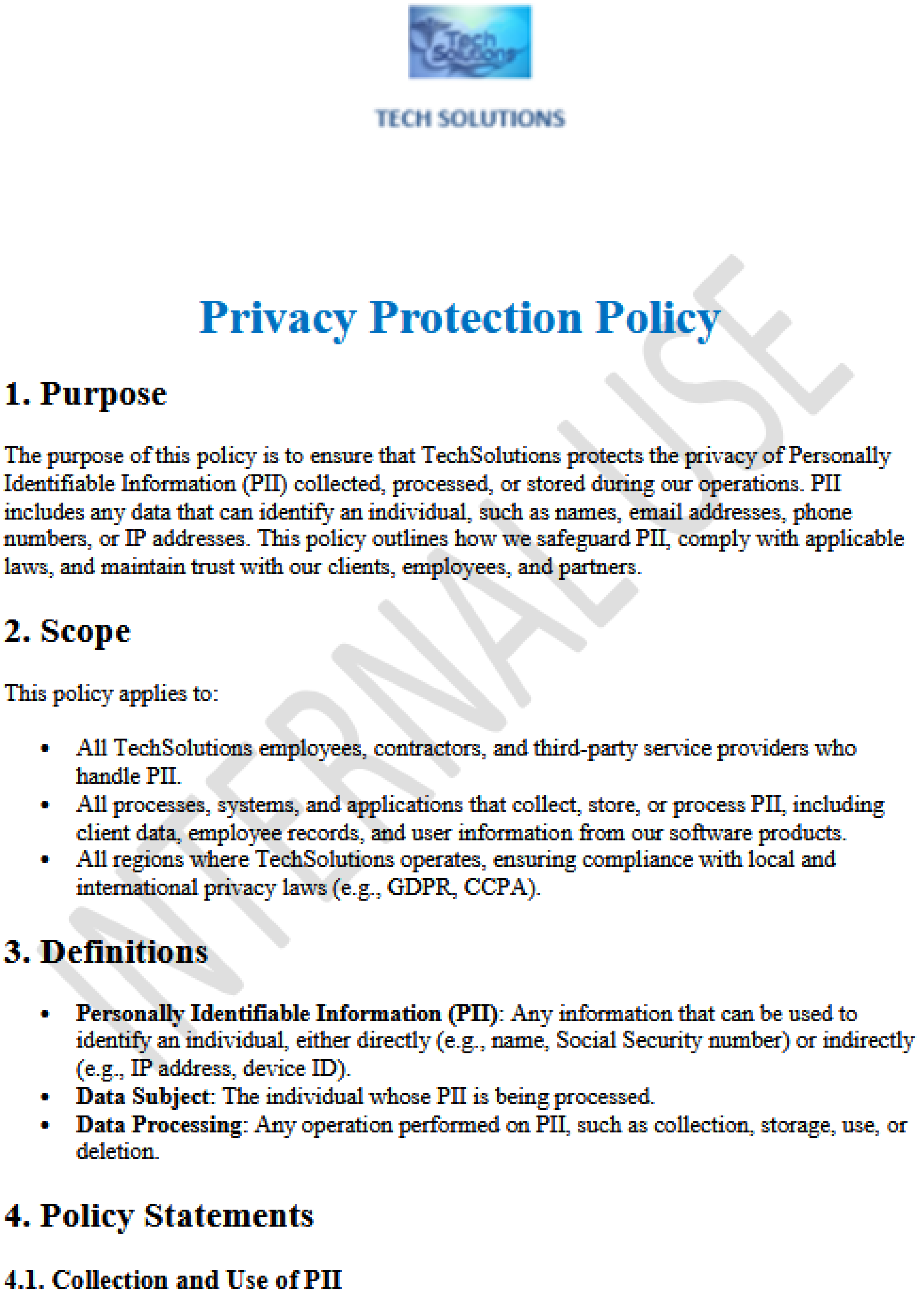
  Technical measure: Your store uses a secure website (HTTPS) and encrypts customer data in the database so hackers can’t read it.

  Organizational measure: Only Sarah and one other employee can access customer data, and they must use strong passwords and log out after use.

Control evidence:

Checks to be performed	Evidence
➢ Whether a specific privacy and personal data protection policy and associated procedures are developed and implemented ➢ If a Data Protection Officer (DPO) is appointed ➢ Whether the DPO provides guidance to staff, service providers and other interested parties on their individual responsibilities ➢	➢ Specific privacy protection policies and procedures ➢ Decision to appoint the DPO

1.12 Practical Application of Clause 5.34: Case Study: ”Tech Solutions”



TECH SOLUTIONS

Privacy Protection Policy

1. Purpose

The purpose of this policy is to ensure that TechSolutions protects the privacy of Personally Identifiable Information (PII) collected, processed, or stored during our operations. PII includes any data that can identify an individual, such as names, email addresses, phone numbers, or IP addresses. This policy outlines how we safeguard PII, comply with applicable laws, and maintain trust with our clients, employees, and partners.

2. Scope

This policy applies to:

- All TechSolutions employees, contractors, and third-party service providers who handle PII.
- All processes, systems, and applications that collect, store, or process PII, including client data, employee records, and user information from our software products.
- All regions where TechSolutions operates, ensuring compliance with local and international privacy laws (e.g., GDPR, CCPA).

3. Definitions

- **Personally Identifiable Information (PII)**: Any information that can be used to identify an individual, either directly (e.g., name, Social Security number) or indirectly (e.g., IP address, device ID).
- **Data Subject**: The individual whose PII is being processed.
- **Data Processing**: Any operation performed on PII, such as collection, storage, use, or deletion.

4. Policy Statements

4.1. Collection and Use of PII

- TechSolutions collects PII only when necessary for legitimate business purposes, such as providing software services, managing employee records, or responding to client inquiries.
- PII will not be used for purposes other than those communicated to the data subject unless consent is obtained.
- **Example**: When a client signs up for our software, we collect their name and email to create an account but do not use this data for marketing unless they agree.

4.2. Consent and Transparency

- Data subjects will be informed about what PII is collected, why it is needed, and how it will be used before collection.
- Consent will be obtained where required by law (e.g., for marketing emails or sensitive data like health information).
- **Example**: Our website includes a pop-up that explains we collect email addresses for newsletters and requires users to check a consent box.

4.3. Data Minimization

- TechSolutions collects only the minimum PII required to achieve the intended purpose.
- **Example**: For a software demo, we ask for a name and email but not unnecessary details like a home address.

4.4. Data Security

- Technical and organizational measures will be implemented to protect PII from unauthorized access, loss, or disclosure.
- **Technical Measures**:
    - Encrypt PII during transmission (e.g., using HTTPS) and storage (e.g., AES-256 encryption).
    - Use firewalls and intrusion detection systems to protect databases.
    - Implement multi-factor authentication (MFA) for systems accessing PII.
- **Organizational Measures**:
    - Restrict access to PII to authorized personnel only, based on their role.
    - Conduct regular employee training on PII protection and phishing prevention.
    - Maintain an incident response plan for data breaches.
- **Example**: Client data in our CRM system is encrypted, and only the sales team can access it with secure logins.

4.5. Data Sharing and Third Parties

- PII will not be shared with third parties unless necessary (e.g., for payment processing) and only with data subjects' consent or legal obligation.
- Third-party vendors (e.g., cloud providers) must sign data processing agreements to ensure PII protection.
- **Example**: We use a secure cloud provider for backups, and they are contractually obligated to follow GDPR and encrypt data.

4.6. Data Retention and Deletion

- PII will be retained only for as long as necessary to fulfill the purpose for which it was collected or as required by law.
- When no longer needed, PII will be securely deleted or anonymized.
- **Example**: Client contact details are deleted 12 months after a project ends, unless required for tax purposes.

4.7. Data Subject Rights

- Data subjects have the right to access, correct, delete, or restrict the use of their PII, subject to legal requirements.
- Requests from data subjects will be processed within 30 days.
- **Example**: If a client emails us to delete their account data, our privacy officer verifies the request and removes the data from our systems.

5. Roles and Responsibilities

- **Privacy Officer**: TechSolutions appoints a Privacy Officer to oversee PII protection, ensure compliance with this policy, and provide guidance to staff and vendors.
  - Responsibilities include:
    - Reviewing and updating this policy annually.
    - Training employees on PII handling procedures.
    - Investigating and responding to data breaches or complaints.
  - Contact: privacy@techsolutions.com
- **Employees**: All employees must follow this policy and report any suspected PII breaches to the Privacy Officer immediately.
- **Third Parties**: Vendors and partners must comply with this policy and applicable laws when handling TechSolutions' PII.

6. Procedures for PII Protection

The following procedures ensure consistent handling of PII:

1. **Data Collection**:
   - Use secure forms (e.g., HTTPS websites) to collect PII.
   - Clearly state the purpose of collection and obtain consent where needed.
2. **Data Storage**:
   - Store PII in encrypted databases or secure cloud platforms.
   - Limit access to authorized personnel via role-based access controls.
3. **Data Processing**:
   - Process PII only for the stated purpose and within secure systems.
   - Regularly audit systems to detect unauthorized access.
4. **Data Sharing**:
   - Share PII only with approved third parties under a data processing agreement.
   - Use secure methods (e.g., encrypted file transfers) for sharing.
5. **Data Deletion**:
   - Delete PII using secure methods (e.g., overwriting data) when no longer needed.

    - Document deletion for audit purposes.
6. **Incident Response**:
    - Report suspected breaches to the Privacy Officer within 24 hours.
    - Notify affected data subjects and authorities as required by law (e.g., GDPR's 72-hour rule).

7. Compliance with Laws and Regulations

- TechSolutions complies with all applicable privacy laws, including but not limited to:
    - General Data Protection Regulation (GDPR) for European clients.
    - California Consumer Privacy Act (CCPA) for California residents.
    - Other local regulations based on operational regions.
- The Privacy Officer monitors changes in laws and updates procedures accordingly.
- **Example**: For GDPR compliance, we allow European clients to request data deletion and provide a downloadable copy of their PII.

8. Training and Awareness

- All employees receive annual training on this policy, PII protection, and relevant laws.
- New hires complete privacy training within their first week.
- Third-party vendors receive a summary of this policy and must acknowledge compliance.
- **Example**: We hold quarterly workshops to teach staff how to recognize phishing emails that could compromise PII.

9. Monitoring and Review

- The Privacy Officer conducts quarterly audits of PII handling processes to ensure compliance.
- This policy is reviewed and updated annually or when significant changes occur (e.g., new laws or technologies).
- Non-compliance with this policy may result in disciplinary action, up to and including termination.

10. Contact Information

For questions, concerns, or to exercise data subject rights, contact:

- **Privacy Officer**: Jane Doe
- **Email**: privacy@techsolutions.com
- **Phone**: +1-800-555-1234
- **Address**: TechSolutions, 123 Innovation Drive, Tech City, TC 12345

11. Effective Date

This policy is effective as of May 7, 2025, and supersedes all previous privacy policies.

Approval
Name: John Smith, CEO
Date: May 7, 2025