YouTestMe

Information Security Policies

Table of Contents

1 Introduction

As the world becomes increasingly digitized and interconnected, the importance of information security has become more critical than ever. With personal data being the lifeblood of many organizations, protecting that information has become a paramount concern. Without proper information security policies and protocols in place, organizations are at risk of data breaches, cyber attacks, and other security threats that can result in significant financial losses, damage to reputation, and even legal liability.

The careful usage of personal data is one of the most important considerations for any organization. Whether it is customer data or employee data, personal information must be treated with the utmost care and respect. This means implementing robust security measures, including access controls, encryption, and monitoring, to ensure that personal data is only accessed by authorized personnel and is not vulnerable to external threats.

In addition to protecting personal data, organizations must also protect themselves from attacks and malware. Cyber attacks are becoming increasingly sophisticated and targeted, and organizations must be proactive in their defense against these threats. This includes implementing effective firewalls, antivirus software, and intrusion detection systems, as well as training employees on best practices for avoiding phishing scams and other common attack vectors.

Overall, the importance of information security policies cannot be overstated. By taking a proactive approach to information security, organizations can safeguard their data, protect their reputation, and avoid potentially devastating security breaches. In this document, we will outline the key policies and protocols that organizations should implement to ensure the careful usage of personal data and protection from attacks and malware.

2 Scope of Policy

The Information Security Policies document applies to all employees, including temporary employees, interns, and contractors, who have access to company YouTestMe's information systems and data. This policy is designed to protect the organization from data loss, leakage of personal information, and to ensure business continuity with minimum downtime.

The policy covers a wide range of information security issues, including but not limited to, access controls, data classification and handling, incident management, network and system security, and user responsibilities. It applies to all information systems, including those owned, leased, or managed by the organization.

The policy is intended to provide a framework for the implementation of information security controls that are consistent with legal, regulatory, and contractual requirements. It sets out the responsibilities of employees and contractors in maintaining the confidentiality, integrity, and availability of information.

This policy is intended to complement other policies and procedures in place, such as the Acceptable Use Policy, and is subject to periodic review and update to ensure that it remains current and effective in addressing new and emerging threats to information security.

By implementing this policy, company YouTestMe aims to minimize the risk of security breaches and protect the organization's reputation, financial stability, and compliance with legal and regulatory requirements.

3 Objectives

3.1 Infrastructure Availability

The objective of this Information Security Policy is to ensure the availability of company YouTestMe's infrastructure by mitigating security issues that may cause disruption or downtime. By implementing robust security measures and protocols, the organization aims to prevent security incidents that can impact the availability of critical systems and services. The policy outlines the responsibilities of employees and contractors in maintaining the security of information systems, and provides guidelines for incident response and recovery in the event of a security breach. By achieving this objective, the organization can ensure business continuity and maintain customer trust and confidence.

3.2 Protection of Personal Information

The objective of this Information Security Policy is to protect the personal information of clients and employees of company YouTestMe. The policy aims to ensure that personal information is collected, processed, stored, and disposed of in a secure and confidential manner, and that access to personal information is limited to authorized personnel only. The policy outlines the responsibilities of employees and contractors in protecting personal information, and provides guidelines for incident response and reporting in the event of a data breach. By achieving this objective, the organization can maintain the trust and confidence of its clients and employees, and comply with applicable laws and regulations related to the protection of personal information.

4 Roles and Responsibilities

Next roles are responsible for maintaining security levels and procedures in security framework:

- **Information Security Manager (ISM)**: Responsible for overseeing the implementation and maintenance of the information security management system (ISMS) based on ISO 27001.
- **Security Officer (SO)**: Develops and implements security policies, procedures, and guidelines. Monitors compliance with security controls, manages security incidents, and provides security awareness training.
- **Risk Manager (RM)**: Identifies, assesses, and manages information security risks. Conducts risk assessments, defines risk treatment plans, and monitors risk mitigation measures.
- **System Administrator (SA)**: Manages the IT infrastructure, configures and monitors security controls, implements access controls, and maintains system backups.
- **Application Developer (AD)**: Ensures secure coding practices, conducts application security testing, and collaborates with the security officer and system administrators for secure application deployment.
- **Internal Auditor (IA)**: Conducts regular audits to assess the effectiveness and compliance of the ISMS with ISO 27001 requirements.
- **Human Resources (HR)**: Assists in conducting background checks, implementing security awareness training programs, and addressing employee security-related concerns.
- **Legal and Compliance Officer(LCO)**: Ensures compliance with legal and regulatory requirements related to information security.
- **Members (M)**: Every company member with any level of access to information or equipment. Informs management about security issues in the system.

Assessment levels for responsibilities are:

- **R** - responsible - Role performing a task or controls that the task is performed correctly.
- **A** - approves -
- **C** - consulted
- **I** - informed

4.1 Roles Matrix

Roles / Responsibilities	ISM	SO	RM	SA	AD	IA	HR	LCO	M
Defining and maintaining the information security policies.	A	R	C	C	C			C	I
System Hardening and Configuration	I	A		R	C				I
User Account Management	A	A		R			C	C	I
Access Control and Privilege Management	A	A	C	R			C		I
System Patching and Updates	I	C		R		I			
System Monitoring and Logging	C	I	I	R					
Backup and Recovery	A	I		R	C				
Incident Response and Reporting	A	C		R					
Virus and Malware Protection				R					
Disaster Recovery and Business Continuity				R					
Secure Coding Practices	A	I		C	R				
Application Vulnerability Management	A	I		C	R				
Secure Application Configuration Management	A	I		C	R				
Secure Authentication and Authorization in Application	A	I		C	R				
Application Data Protection	A	I		C	R				
Secure Third-Party Libraries and Components	A	I		C	R				
Secure Deployment Practices	A	I		C	R				
Secure Testing and Quality Assurance	A	I		C	R				
Secure Application Incident Response	A	I		C	R				
Employee Onboarding and Offboarding	I	I					R	C	
Security Awareness and Training	I	A		C			R		
Policy Enforcement	I	A		C			R		
Access Control Management	I	A		R			C		

5 Employees Security Policies

This Employees Security Policies outlines the guidelines and procedures for onboarding, data usage, and cybersecurity awareness at YouTestMe. It is designed to ensure compliance with ISO 27001 and promote the protection of sensitive data throughout the employment process. All employees are required to read, understand, and adhere to this policy.

5.1 Onboarding Process

1. **Data Usage Consent** - During the onboarding process, all employees must sign a consent form acknowledging that their personal data will be used solely for employment-related purposes. This consent includes data collection, processing, storage, and sharing in compliance with applicable privacy laws and regulations.
2. **Employee Data Protection** - YouTestMe is committed to safeguarding employee data throughout the onboarding process. Access to personal information will be granted only to authorized personnel who require it for legitimate business purposes. Appropriate security measures will be implemented to prevent unauthorized access, disclosure, or alteration of employee data.

5.2 Training on Cybersecurity and Data Protection

1. **Cybersecurity Awareness Training** - All employees will receive mandatory training on cybersecurity best practices and data protection. This training will cover topics such as phishing, password security, safe browsing, email etiquette, and reporting security incidents. The objective is to enhance employees' understanding of potential risks and equip them with the knowledge to mitigate those risks.
2. **Responsible Data Handling** - Employees will be educated on the importance of responsible data handling, including the secure storage and transmission of sensitive information. They will be instructed to adhere to the organization's data protection policies and procedures, ensuring that data is accessed, used, and shared only on a need-to-know basis and in accordance with the applicable privacy regulations.
3. **Reporting Security Incidents** - Employees will be provided with clear guidelines on reporting security incidents promptly. They should notify the designated IT or security personnel immediately if they suspect or become aware of any cybersecurity threats, data breaches, or potential vulnerabilities. Timely reporting will enable prompt investigation and remedial actions to mitigate the impact of security incidents.

5.3 Compliance Monitoring and Continuous Improvement

1. **Compliance with ISO 27001** - YouTestMe is committed to maintaining compliance with ISO 27001 standards. Regular audits and assessments will be conducted to monitor adherence to the HR policy and related controls. Any non-compliance or gaps identified during audits will be addressed promptly.
2. **Continuous Improvement** - The HR policy and associated procedures will be periodically reviewed and updated to reflect changes in regulations, technologies, and business requirements. Feedback from

employees regarding the effectiveness and usability of the policy will be sought to drive continuous improvement.

5.4 Policy Acknowledgement

By signing the HR Policy Acknowledgement form, employees confirm that they have read, understood, and agreed to comply with the HR policy, including data usage consent, cybersecurity awareness training, and responsible data handling. Failure to comply with the policy may result in disciplinary action, up to and including termination of employment.

5.5 Policy Review

This HR policy will be reviewed annually or as required to ensure its continued relevance and effectiveness in protecting employee data and promoting cybersecurity awareness.

5.6 Policy Distribution

This HR policy will be distributed to all employees upon onboarding and made available on the company's intranet or HR portal for easy access.

6 Personal Information Policies

1. **Data Minimization**: YouTestMe follows a strict data minimization approach, ensuring that only necessary and relevant personal information is collected and processed. Unnecessary data is not retained, reducing the risk of unauthorized access or misuse.
2. **Consent and Control**: YouTestMe respects individual privacy rights and seeks explicit consent for the collection, use, and disclosure of personal information. Individuals have the right to withdraw their consent at any time and can exercise control over their personal data, including the ability to access, correct, or delete their information.
3. **Security Safeguards**: YouTestMe implements appropriate technical and organizational measures to protect personal information against unauthorized access, alteration, disclosure, or destruction. These safeguards include encryption, access controls, regular security assessments, and employee awareness and training programs.
4. **Data Retention**: YouTestMe retains personal information only for the duration necessary to fulfill the purposes for which it was collected, unless legal requirements dictate otherwise. Personal data is securely disposed of when it is no longer needed.
5. **Incident Response**: YouTestMe maintains an incident response plan to address and mitigate any breaches or unauthorized access to personal information. This plan includes timely identification, containment, investigation, and notification procedures to protect individuals and comply with legal obligations.
6. **Compliance and Accountability**: YouTestMe regularly monitors and reviews its personal information protection practices to ensure compliance with applicable privacy laws and regulations. We have designated responsible individuals and processes in place to address privacy-related concerns and provide guidance to employees.
7. **Education and Awareness**: YouTestMe promotes privacy awareness among its employees, customers, and stakeholders through training programs, awareness campaigns, and communication channels. This ensures a culture of privacy protection and responsible personal information handling.

7 Access Control

1. **Principle of Least Privilege**: Employees should be granted only the necessary access privileges required to successfully complete their tasks and responsibilities. Exceptions to this rule are limited to higher management positions.
2. **Access Provisioning**: Access to systems is provided by the respective team leader or system administrators, depending on the specific system. Requests for access must be confirmed by the higher management or the relevant team leader before access is granted.
3. **Role-Based Access Control (RBAC)**: Access privileges for different company roles are defined in the Access Control document. The document outlines the specific access rights and permissions associated with each role, ensuring appropriate access levels are assigned.
4. **Access Termination and Changes**: Access privileges are promptly retracted when an employee's contract is terminated or their position within the company changes. Additionally, if access privileges are shared with multiple members, the authorization parameters for all shared accounts should be changed to ensure accountability and security.

8 Business Continuity and Disaster Recovery

The YouTestMe is committed to ensuring the continuity of its critical business functions and minimizing the impact of disruptions. This policy establishes our approach to business continuity management, which includes the development, implementation, and maintenance of a Business Continuity Management System (BCMS). Our goal is to effectively respond to incidents, maintain essential operations, and restore normal business activities in a timely manner.

8.1 Business Impact Analysis

1. **Regular Review**: Business Impact Analysis (BIA) will be conducted at defined intervals to ensure ongoing risk reduction and identification of critical vulnerabilities affecting uninterrupted business functions. Findings from the BIA will be used to enhance the organization's resilience by addressing weaknesses and implementing necessary improvements.
2. **Recovery Objectives**: Define specific recovery time objectives for services and applications based on importance and service level agreements, and acceptable data loss levels for services and applications in the event of a disaster.
3. **Dependency Analysis**: Identify critical dependencies between systems, processes, and resources to understand potential impacts and implement mitigation measures.
4. **Documentation and Maintenance**: Document BIA findings, including critical functions, dependencies, and recovery objectives. Regularly review and update the documentation.
5. **Testing and Validation**: Conduct regular testing and validation to ensure effective recovery procedures, meet defined recovery objectives, and learn from the exercises.

8.2 Incident Response and Management

8.2.1 Incident Response Team:

1. **Composition**: The incident response team includes System Administrators, Developers, and relevant personnel with defined roles and responsibilities.
2. **Readiness**: Team members receive training and drills to ensure readiness for effective incident response.

8.2.2 Incident Response Procedure:

1. **Comprehensive Procedure**: The procedure covers all steps of incident response, including identification, containment, eradication, recovery, and lessons learned.
2. **Guidelines**: Provide specific instructions for handling different types of incidents for a consistent and efficient response.

8.2.3 Incident Reporting:

1. **Reporting**: All incidents, regardless of severity, must be promptly reported according to the procedure.
2. **Information Collection**: Reports should include essential details such as incident time, affected systems, and initial impact assessment.

3. **Continuous Improvement**: Incident reports are used to improve the incident response procedure and management practices.

8.2.4 Testing and Exercising:

1. **Frequency and Coverage**: Regularly test and exercise incident response procedures to assess readiness and identify areas for improvement. Cover various scenarios through tabletop and simulated exercises.
2. **Lessons Learned**: Review and document lessons learned from testing sessions. Incorporate findings into the incident response procedure and provide additional training as needed.

8.3 Disaster Recovery Management

1. **Backup Schedule**: YouTestMe's security policy includes establishing a regular backup schedule that aligns with the criticality and sensitivity of the data, ensuring consistent data protection.
2. **Backup Methods**: YouTestMe's security policy outlines the selection and utilization of appropriate backup methods, such as full backups, incremental backups, or differential backups, based on the specific data requirements.
3. **Storage Locations**: YouTestMe's security policy mandates the identification of secure offsite storage locations for backup media, aiming to protect against physical disasters or incidents and maintain data integrity.
4. **Disaster Scenario Plans**: YouTestMe's security policy requires the creation of comprehensive disaster scenario plans that consider various outage or disaster situations. These plans are developed based on previous experiences and lessons learned, ensuring effective response and recovery measures are in place.