Academic Year: 2024-25 Sap Id: 60003220045

Department of Information Technology

COURSE CODE: DJS22ITL6015 **DATE: 18-02-2025**

COURSE NAME: ISIG Laboratory **CLASS: T. Y. B.Tech**

NAME: Anish Sharma **DIV:** IT1-1 **ROLL:** I011

Experiment No. 4

CO/LO: Describe the types of support that an information system can provide to each functional area of the organization.

Information Security Policy Development

AIM / OBJECTIVE: To create an effective information security policy for an organization
(Bank, IT Industry, Government and public sector companies like HAL, ISRO, Big Hospitals, Pharmaceutical companies, telecom companies, e-commerce and retail industries, education and universities, insurance companies, aviation and transportation, energy and power sector).

Tools Used: Policy templates, ISO/IEC 27001 guidelines.

Outcome: A robust security policy document covering data privacy, cybersecurity, and compliance.

Objective:

The goal of developing an information security policy is to establish a structured approach to protecting an organization's data, systems, and IT infrastructure. The policy sets the foundation for ensuring confidentiality, integrity, and availability of information while addressing cybersecurity threats, data privacy concerns, and compliance requirements.

Tools Used:

Department of Information Technology

1. **Policy Templates:** Predefined formats that help in structuring policies effectively.
2. **ISO/IEC 27001 Guidelines:** International standards that provide a framework for information security management.

Outcome:

The final output is a comprehensive **Information Security Policy Document** that ensures the organization follows best security practices, mitigates risks, and complies with regulatory standards.

Introduction

Walmart Inc., a global leader in retail and e-commerce, is committed to safeguarding the confidentiality, integrity, and availability of its information assets. This policy establishes a robust framework to protect customer data, supply chain systems, financial transactions, and IT infrastructure against cyber threats, unauthorized access, and data breaches. Aligning with Walmart's mission to deliver trusted services, this policy ensures compliance with international regulations and fosters a culture of security awareness across all operations.

Scope

This policy applies to:

- **All associates, contractors, consultants, temporary workers, and third-party vendors** interacting with Walmart systems.
- **All information assets**, including hardware, software, cloud services, networks, IoT devices, and data (e.g., customer PII, payment details, inventory systems).
- **Global operations**, including retail stores, distribution centers, e-commerce platforms (Walmart.com, Sam's Club), and corporate offices.

Information Security Objectives

1. **Confidentiality**: Restrict access to sensitive data to authorized personnel only.

2. **Integrity**: Ensure accuracy and reliability of data across all systems.
3. **Availability**: Maintain uninterrupted access to critical systems for customers and associates.
4. **Compliance**: Adhere to global regulations (e.g., GDPR, CCPA, PCI-DSS, SOX) and industry standards (ISO 27001, NIST).

Information Security Objectives

Walmart Inc. is committed to maintaining the highest levels of security across all aspects of its operations. The primary objectives of this Information Security Policy are:

1. Confidentiality

Walmart's commitment to confidentiality ensures that sensitive information remains protected from unauthorized access or disclosure. This includes:

- **Customer Data:** Ensuring that personally identifiable information (PII), financial details, and purchase history are encrypted and only accessible to authorized personnel.
- **Internal Data:** Protecting employee information, internal communications, and business strategies from external or internal threats.
- **Trade Secrets:** Safeguarding proprietary company data, algorithms, and supply chain information critical to competitive advantage.

Key Actions:

- Enforce strict access control policies.
- Encrypt sensitive data both in transit and at rest.
- Establish security measures around data sharing practices to mitigate unauthorized disclosures.

2. Integrity

The integrity objective ensures that information remains accurate, reliable, and free from unauthorized modifications. This includes:

- **Data Consistency:** Preventing unauthorized alterations of customer orders, inventory records, financial transactions, and other critical business data.

- **Transaction Verification:** Ensuring that all financial and purchase transactions are accurately recorded and reflect the true nature of the exchanges.
- **Audit Trails:** Implementing robust logging mechanisms to track changes made to critical systems, ensuring that any discrepancies can be traced back to their source.

Key Actions:

- Employ automated systems for real-time monitoring of data integrity.
- Regularly perform data validation checks to ensure consistency.
- Use version control for critical documents and software to prevent tampering.

3. Availability

Ensuring that Walmart's digital and physical assets, systems, and services are readily accessible to authorized users when needed is a core objective. This includes:

- **System Uptime:** Maintaining reliable access to e-commerce platforms, point-of-sale systems, inventory management, and other critical operations.
- **Disaster Recovery:** Ensuring that business-critical services can be quickly restored in the event of a system failure, data breach, or disaster scenario.
- **Business Continuity:** Minimizing downtime and operational disruptions, ensuring customers and associates experience minimal impact from security incidents.

Key Actions:

- Implement redundancy and backup systems to ensure business continuity.
- Establish disaster recovery plans, regularly test failover systems, and ensure high availability for critical applications.
- Monitor system performance and proactively address vulnerabilities or bottlenecks that could affect system availability.

4. Compliance

Ensuring that Walmart adheres to international laws, regulatory frameworks, and industry standards is critical to maintaining a trusted business environment. This includes:

- **Privacy Regulations:** Complying with laws governing the handling of personal data, such as GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), and other regional privacy laws.
- **Industry Standards:** Adhering to standards like ISO/IEC 27001, PCI-DSS (Payment Card Industry Data Security Standard), and NIST (National Institute of Standards and Technology) frameworks to safeguard data.
- **Financial and Reporting Regulations:** Complying with regulations such as SOX (SarbanesOxley Act), which requires accurate reporting of financial transactions.

Key Actions:

- Conduct periodic assessments and audits to verify compliance with industry standards and regulatory frameworks.
- Maintain an internal compliance team that stays up-to-date on changes in relevant laws and regulations.
- Implement regular training and awareness programs to ensure all associates understand their roles in maintaining compliance.

Roles & Responsibilities

Role	Responsibilities
Associates	Report incidents via GSOC; adhere to password policies.
IT Security Team	Monitor threats via AI-driven SIEM; manage firewalls/encryption.
Global CISO	Oversee policy implementation; report to the Board on cyber risks.
Vendor Manager	Conduct third-party due diligence; enforce SLAs.

Policy Enforcement & Review

- **Annual Review**: Updated to reflect emerging threats (e.g., ransomware, AI-driven attacks).
- **Non-Compliance**: Disciplinary action, up to termination; vendors face contract termination.
- **Audits**: Internal audits quarterly; external audits for ISO 27001 recertification.

References

- ISO/IEC 27001:2013
- NIST Cybersecurity Framework
- PCI-DSS v4.0
- Walmart Global Compliance Handbook

Conclusion

This policy underscores Walmart's commitment to securing its digital ecosystem, enabling safe customer experiences and operational resilience. By aligning with global standards and fostering proactive threat management, Walmart ensures trust across its 2.3 million associates and 240 million weekly customers.