Marie Madeleine Anita Bekono

Old Dominion University

CYSE-300

Joe Kovacic

09/17/2023

## Key Security Policy Issues

Information security regulations are vital to protecting sensitive data and systems within an organization. For an enterprise with on-premises infrastructure hosting internet, software, and database servers that shop pretty exclusive records, the safety policy ought to deal with critical risks and establish required controls. This paper will discuss five crucial regions that want to be protected inside the security policy so one can protect the touchy information and technology assets. These include imposing proper admission to controls, encrypting and securing statistics, hardening server systems, planning incident reaction techniques, and keeping compliance with policies. By developing policies around those issues, the agency can lessen vulnerabilities, respond to threats, and ensure the confidentiality, integrity, and availability of essential business structures and records. The policy also communicates safety requirements and necessities to personnel, facilitating the adoption of prudent practices company-wide.

1. Access Control

The policy must specify who can access which data and systems and under what circumstances. For the databases storing sensitive data, access should be strictly limited to select official or authorized personnel based on their roles and responsibilities. Robust authentication techniques like multifactor authentication ought to be required to access sensitive systems (Duggineni, 2023). The policy needs strategies for granting, converting, and revoking access rights.

A role-based access control (RBAC) model has to be used to limit access to authorized users only. Employees must be granted device and data access strictly per their activity roles and duties on a need-to-know foundation. Access review methods must be mounted, requiring managers to assess and validate employees' access to privileges periodically. Any change in user roles or employment fame needs to initiate an assessment manner.

For third-party vendors and contractors desiring transient get right of entry, extra controls need to be applied, including restricting privileged instructions, tracking activities, and ensuring get entry to receives revoked right now after completion of work. All user access activities and entitlements should be logged to enable required auditing. Multifactor authentication must be applied for remote access to infrastructure hosting sensitive data. The policy has to have straightforward tactics for approving, provisioning, reviewing and revoking admission in all situations.

2. Data Protection

Since the databases include sensitive information, the policy desires to mandate sturdy protections like encryption for information at rest and in transit. It needs to classify data sensitivity tiers, require corresponding protections, and get access to regulations for every level. Backups should be encrypted and access secured. Data retention and destruction suggestions need to be installed.

The policy should mandate encryption at rest and in transit for sensitive data. Databases containing exclusive purchaser, monetary, or intellectual assets data must be encrypted using solid standards like AES-256. Servers hosting sensitive data should have encrypted storage. Network traffic containing sensitive data should be encrypted through TLS, SSL, or VPNs. Procedures for cryptographic key control need to be set up (Rainer et al., 2022). Data category suggestions should be created to outline protection necessities and get the right of entry to rights for diverse ranges of sensitivity. Maximum data retention periods must be defined per type level, with expired data securely disposed of or deleted. Regular audits must check for unencrypted sensitive information and ensure compliance with retention/destruction protocols. Data loss prevention and rights

control solutions must also be considered to prevent unauthorized entry to, copying, or transmitting sensitive data.

3. System Security

Servers, endpoints, and network infrastructure must be hardened to the field protection standards. This includes keeping structures patched and updated, configuring firewalls and intrusion detection accurately, proscribing needless services/ports, and many others. Password regulations should require solid and unique passwords to be changed frequently. Multifactor authentication must be used in any place possible.

Server and device protection have to follow field quality practices and requirements. Operating structures, software programs, and applications have to be stored up to date with the trendy supplier patches. Unnecessary open ports and services must be turned off to reduce attacks. Firewalls, intrusion detection/prevention systems, and endpoint security tools must be implemented to reveal threats and block malicious right of entry. Audit logging should be enabled to offer interest trails. Vulnerability scanning ought to regularly look at structures for dangers that want remediation. The policy must reference specific hardening suggestions and check out necessities to ensure robust safety baselines throughout on-premises infrastructure.

4. Incident Response

The policy must outline strategies to detect, respond to, and recover from security incidents like breaches or data leaks. Roles and responsibilities must be defined at the side of methods for threat evaluation, evidence amassing, containment, eradication, recovery, and external communications/disclosures if required through regulation. Post-incident evaluations should identify lessons learned.

The incident response plan must designate roles and obligations for detecting, evaluating, containing, remedying, and communicating security incidents. Evidence amassing and forensic strategies want to be described to guide potential legal prosecution. Steps for assessing harm, restoring data, and reusing structures online must be mentioned (Whitman et al., 2021). Post-incident analysis ought to identify root causes, training found, and policy updates to prevent recurrence. Public family members steering concerning external communications and disclosures must be set up for essential incidents to maintain public self-belief. The plan has to be examined through simulations to validate its effectiveness. Clean, tested response methods facilitate rapid, organized mitigation of adverse occasions and breaches.

5. Compliance

Relevant safety standards, guidelines, and contractual responsibilities ought to be identified. Processes for ordinary security assessments and audits ought to be carried out to ensure continuous compliance. Violations of policy must bring about proportionate disciplinary action. Confidential reporting of non-compliance ought to be facilitated.

The policy needs to discover applicable safety standards and policies the organization should adhere to, primarily based on its enterprise and information types. These may additionally encompass frameworks like ISO 27001, PCI DSS, HIPAA, and diverse records privacy legal guidelines. Internal audits must periodically review and validate compliance, with effects stated to senior management. Violations of policy have to result in suitable disciplinary measures. Confidential reporting mechanisms must be provided for personnel to file non-compliance without worrying about retaliation. Security focus training for staff should include schooling on policy and compliance responsibilities. Maintaining compliance demonstrates the enterprise's dedication to security and protects its reputation.

In conclusion, an adequate record of safety coverage is the inspiration for protecting sensitive systems and data in an organization. For an organization with on-premises infrastructure containing confidential customer information, the policy must address access control, data/Information safety, machine hardening, incident response, and compliance. Implementing robust controls in those key areas reduces vulnerabilities, permits proper responses to threats, and safeguards the integrity and availability of critical enterprise systems and data. The policy translates excellent security practices into actionable standards and procedures for the corporation to follow. Corporations can securely operate sensitive data and meet data safety obligations with a comprehensive regional policy.

## References

Duggineni, S. (2023). Impact of Controls on Data Integrity and Information Systems. *Science and Technology*, *13*(2), 29-35.

Rainer, R. K., & Prince, B. (2022). *Introduction to information systems: Supporting and transforming business*. John Wiley & Sons.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.