Training and Awareness

Diné College Information Technology

Michael Morrow

Revision History

Version Number	Revision Date
1.0	10/2/2024

Table of Contents

1. Purpose

The purpose of this policy is to provide clear guidelines for developing and implementing an effective information security training and awareness program. This policy aims to ensure all employees are equipped with the knowledge and skills necessary to protect the organization's information systems, data, and assets from security threats and vulnerabilities.

2. Scope

This policy applies to all employees, contractors, and third-party personnel who have access to the organization's information systems, data, or assets. It covers all aspects of information security training and awareness, including initial onboarding, periodic refresher courses, and ongoing awareness activities. The policy encompasses all forms of training delivery, including in-person sessions, online courses, and written materials.

3. Roles and responsibilities

The following roles are responsibilities outline the ownership and actions held by stakeholders in the response process.

Chief Information Security Officer (CISO)

The CISO is responsible for overseeing the development and implementation of the information security training and awareness program. This includes ensuring the training program aligns with the organization’s overall information security strategy, as well as reviewing and approving training materials and content updates.

Information Security Team

The Information Security Team is tasked with creating and updating information security training materials, conducting training sessions, and ensuring their effectiveness. They monitor compliance with the training and awareness policy and provide support and answer questions related to information security practices.

Department Heads

Department heads are responsible for ensuring their team members complete the required information security training and adhere to the practices outlined in the training within their departments. They address any non-compliance issues and report them to the Information Security Team.

Employees

Employees should participate in all required information security training sessions, understand and follow the information security policies and procedures, and apply the knowledge gained from the training to protect the organization’s information assets. They are also responsible for reporting any security incidents or concerns to the appropriate personnel

4. Training Program Structure

The training program structure provides a comprehensive framework for delivering information security education and awareness across the organization. This program is designed to ensure that all employees, from new hires to seasoned staff, understand their responsibilities in maintaining the security of the organization's information assets.

Initial Onboarding Training

New employees should receive detailed information security training as part of their onboarding process. This training should introduce them to the organization's security policies, procedures, and best practices. Topics should include an overview of data protection, password management, secure use of mobile devices, and the importance of reporting security incidents.

Periodic Refresher Courses

To ensure that all employees stay current with the latest information security practices and threats, mandatory refresher courses should be conducted annually. These courses should revisit core security concepts and introduce any updates or changes to the organization's security policies.

Specialized Training

Certain roles within the organization may require more in-depth security training. Specialized training sessions should be provided for employees with specific security responsibilities or those who handle sensitive information. This may include IT staff, system administrators, and employees in high-risk departments such as finance or `HR.

Role-Based Training

Training should be tailored to the various levels of responsibility and access within the organization. For example:

- Executives and Senior Management: Focus on strategic aspects of information security, compliance, and the importance of a security-conscious culture.
- IT and Security Teams: In-depth technical training on managing and mitigating security threats, incident response, and maintaining secure IT infrastructure.
- General Staff: Practical training on everyday security practices, recognizing phishing attempts, and secure handling of organizational data.

Adaptive and Flexible Structure

The training program is designed to be flexible and adaptable. It should be regularly reviewed and updated to reflect changes in the threat landscape, technological advancements, and organizational needs. Feedback from employees should be used to improve the training content and delivery methods.

Interactive and Engaging Format

Training sessions should include a mix of lectures, hands-on activities, and interactive elements such as quizzes and simulations. Real-world scenarios and case studies should be used to make the training more engaging and relatable, helping employees understand the practical applications of security principles.

By establishing a robust and dynamic training program structure, the organization aims to equip all employees with the knowledge and skills necessary to protect its information assets and foster a culture of security awareness.

5. Content of Training

Content of the training should cover a wide range of information security topics, including but not limited to:

- Data protection
- Password management
- Phishing and social engineering
- Secure use of mobile devices
- Incident reporting procedures
- Compliance with relevant laws and regulations

The training should include practical examples and scenarios to help employees understand how to apply security principles in their daily work. The content should be reviewed and updated regularly to reflect current best practices and emerging threats.

6. Frequency of Training

Information security training should be conducted on a regular basis to ensure employees remain aware of current threats and best practices. New employees should receive training during their onboarding process. All employees should participate in mandatory annual refresher courses.

Additional training sessions may be scheduled as needed, particularly in response to new threats, significant changes in technology, or updates to security policies. Specialized training should be provided to employees with specific security responsibilities or those handling sensitive information.

7. Methods of Delivery

The training should be delivered using a variety of methods to accommodate different learning styles and schedules. This includes in-person training sessions, online courses, webinars, and written materials.

Interactive elements such as quizzes, simulations, and hands-on exercises should be incorporated to enhance engagement and retention. The organization should also provide access to a library of resources, including videos, articles, and guidelines, to support ongoing learning and awareness. All training materials should be accessible through the organization’s learning management system.

8. Assessment and Certification

The effectiveness of the information security training program should be measured through assessments and certification processes. After completing each training module, employees should be required to take an assessment to evaluate their understanding of the material. These assessments should consist of multiple-choice questions, scenario-based questions, and practical exercises.

Employees should achieve a passing score to demonstrate their competency in the covered topics. Those who do not pass the assessment should be required to retake the training module and assessment until they meet the required standard.

Upon successful completion of the assessments, employees should receive a certification that acknowledges their understanding and adherence to the organization's information security policies. This certification process should be documented and tracked to ensure compliance and identify areas where additional training may be needed.

9. Ongoing Awareness Activities

To maintain a high level of information security awareness, the organization should implement ongoing awareness activities. These activities should reinforce key security concepts and keep employees informed about the latest threats and best practices.

Regular security newsletters and email updates should be distributed to all employees, highlighting recent security incidents, emerging threats, and tips for maintaining security. Interactive activities such as security-themed quizzes, competitions, and simulations should be organized periodically to engage employees and test their knowledge.

The organization should also observe an annual Information Security Awareness Week, during which various events, workshops, and seminars should be held to promote security awareness. Guest speakers and industry experts may be invited to share insights and experiences.

10. Reporting and Metrics

The organization should implement a robust reporting and metrics system to monitor the effectiveness of the information security training and awareness program. Key performance indicators (KPIs) should be established to measure participation rates, assessment scores, and overall program effectiveness.

Regular reports should be generated to track training completion rates and certification statuses across different departments. These reports should be reviewed by the CISO and senior management to ensure compliance and identify areas for improvement.

Metrics should also include the number of security incidents reported, the speed of incident resolution, and employee feedback on the training program. This data should be analyzed to identify trends, assess the impact of the training, and make informed decisions about future training initiatives.

By maintaining a comprehensive reporting and metrics system, the organization should ensure continuous improvement of the information security training and awareness program, fostering a culture of security and resilience.

Reports and metrics may include:

- Track training completion rates for all employees across different departments.
- Measure assessment scores to evaluate employee understanding of the training material.
- Monitor certification statuses to ensure compliance with information security standards.
- Generate regular reports on participation rates and assessment outcomes.
- Review reports by the CISO and senior management to identify areas for improvement.
- Collect and analyze data on the number of security incidents reported.
- Measure the speed and effectiveness of incident resolution.
- Gather employee feedback on the training program to assess satisfaction and identify gaps.
- Identify trends and patterns in security incidents to inform future training initiatives.
- Use metrics to evaluate the overall impact of the training and awareness program on organizational security posture.

11. Compliance and Penalties

Compliance with the Information Security Training and Awareness Policy is mandatory for all employees, contractors, and third-party personnel. The Compliance Officer should conduct regular audits and spot checks to ensure adherence to the policy. Any instances of non-compliance should be documented and addressed promptly.

Penalties for non-compliance may include additional training sessions, formal warnings, suspension of access to information systems, or, in severe cases, termination of employment. Department heads are responsible for addressing non-compliance within their teams and reporting it to the Information Security Team. Employees are encouraged to report any observed non-compliance or security concerns anonymously.