[Company Logo]

# SECURITY TRAINING POLICY

Security Training is a formal process for educating employees about the internet and computer security. Security Training helps to minimize risk thus preventing the loss of IP, money or brand reputation. An effectiveness training program addresses the cybersecurity mistakes that employees may make when using email, the web and in the physical world, such as tail gaiting or improper document disposal.

Document Owner
Head of IT/Security

## Security Training Policy

For

Company Name

Version : 1.0
Date : 01/01/0000
**Next Review Date :**

**Note: Verify with the Policy Owner if this is the correct and latest version before use.**

## Revision History

| Rev. # | Date | Modification Details | Page# | Suggested By | Reviewed By | Approved By |
|---|---|---|---|---|---|---|
| 1.0 | | First Draft | NA | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# Table of Contents

## Purpose

The company understands that people are often the biggest threat (intentionally or inadvertently) to the security of sensitive information. As such, all users of information systems must be made aware of the security risks associated with their activities and of the applicable federal and agency requirements related to the security of Strategic information systems performing work on behalf of the [Company Name]. Those with significant security responsibilities must be adequately trained to carry out their assigned information security-related duties and responsibilities.

## Scope

This policy applies to:

- **All employees** (full-time, part-time, temporary)
- **Contractors and third-party vendors** with system access
- **Interns and guest workers**
- **Any individual granted access** to [Company]'s information systems, networks, or facilities

Coverage includes:
Digital security awareness (phishing, passwords, data protection)
Physical security protocols (badge access, visitor procedures)
Role-specific training for IT, developers, and leadership
Compliance with industry regulations and standards

## Objective

The policy and associated guidance provide an organized security awareness and training program that will inform the company of relevant and recent security topics.

## Responsibility & Accountability

All Personnel Must:

- Complete mandatory training before system access and annually
- Apply learned security practices in daily work
- Immediately report suspicious activity or security concerns

2. Managers/Supervisors:

- Ensure team members complete training on schedule
- Reinforce security best practices in team workflows
- Escalate persistent non-compliance to HR

3. IT/Security Team:

- Develop and update training content annually
- Conduct phishing simulations and security drills
- Monitor completion rates and follow up with stragglers
- Maintain training records for [X] years

4. Human Resources:

- Enroll new hires in security training during onboarding
- Restrict system access until training is completed
- Address policy violations per disciplinary procedures

5. Executive Leadership:

- Approve resources for security training programs
- Lead by example in completing all required training
- Review annual training effectiveness reports

## Non-Compliance

Any Non-Compliance to this Password Management Policy will be dealt with Disciplinary Action as decided by the organization and respective authorities.

## Exceptions

Not Applicable.

|  |  |  |
|---|---|---|
| [Company Logo] | **CONTROLLED DOCUMENT**<br>**Security Training Policy** | Document: Security Training Policy<br>Developed by:<br>Reviewed by:<br>Approved by: |

## Policy Statement

At [Company Name], everyone plays a role in keeping our information, systems, and workplace safe. This policy ensures all employees, contractors, and third parties receive the training they need to protect our data and recognize potential threats.

## Requirements:

1. Mandatory Training for All:

   - New hires must complete security awareness training before accessing any systems.

   - Annual refresher training is required for everyone.

   - Additional training will be provided when systems change or new risks emerge.

2. Key Training Topics:

   - How to spot phishing scams and report suspicious activity.

   - Best practices for physical and digital security (e.g., secure logins, laptop safety).

   - Recognizing insider threats and unusual system behavior.

   - Role-specific training for IT, developers, and security teams.

3. Ongoing Awareness:

   - Monthly security updates via emails, posters, and team discussions.

   - Practical exercises (like simulated phishing tests) to reinforce learning.

4. Accountability:

   - Training completion is tracked, and records are kept.

   - Failure to comply may result in restricted system access or further action.

Security is a shared responsibility and all must stay informed and vigilant.

**Information Security Training Process**

- Training will be provided during orientation sessions for workforce members and students.
- Training will be classroom-based or web-based.
- Security training records will be maintained in the central training system or in department/school systems.
- The company will develop general awareness training to reinforce awareness of security best practices for all computer users.
- The company will provide security awareness presentations and training opportunities for technical support and management with elevated permissions and administrative responsibilities.

Training will consist of, but is not limited to, the following areas:

- Information Security Policies, Standards, Controls, and Guidance.
- Confidentiality, integrity, and availability of information.
- Security practitioner responsibilities and practices for IT staff and system custodians.
- Practical information security safeguards for faculty, staff, and students.
- User response to suspected security incidents.
- Common security threats and vulnerabilities.
- Information Security best practices.
- Secure use of company networks and information systems.
- Legal and department/school requirements.

## Conclusion

Security is not just an IT issue, it’s a shared responsibility that requires commitment from every individual at [Company Name]. This Security Training Policy ensures that all employees, contractors, and third parties understand their role in protecting our systems, data, and workplace. By providing clear expectations, practical training, and ongoing awareness, a culture of security that adapts to evolving threats is build.

Regular training, accountability measures, and leadership support are essential to maintaining our defenses. Together, can minimize risks, safeguard sensitive information, and uphold [Company Name]’s reputation as a trusted organization.

**Stay alert. Stay informed. Stay secure.**

<<< End of Document >>>