The purpose of this Cybersecurity Awareness and Training Policy is to establish guidelines and procedures for creating a culture of cybersecurity awareness within an organization. This policy outlines the requirements and expectations for educating all employees, contractors, and vendors about cybersecurity risks and best practices to mitigate these risks.

Scope:

This policy applies to all employees, contractors, and vendors who have access to the organization's information systems, networks, and data. All personnel must be aware of the organization's cybersecurity policies, procedures, and guidelines.

Policy:

1. Cybersecurity Awareness Training: All personnel who have access to the organization's information systems, networks, and data must complete cybersecurity awareness training at least once a year. This training must be designed to educate employees on the following topics:

a) Security best practices for handling sensitive data b) Password management c) Phishing awareness d) Malware prevention e) Social engineering prevention f) Mobile device security g) Physical security of information systems and data h) Incident response procedures

1. Reporting Security Incidents: All personnel must report any suspected security incidents immediately to their supervisor, the IT department, or the designated security officer. Incidents may include, but are not limited to, phishing emails, suspicious website pop-ups, or unauthorized access attempts.
2. Password Requirements: All personnel must comply with the organization's password policy. Passwords must be changed every 90 days, and must meet complexity requirements that include a minimum length of eight characters, and the use of a combination of letters, numbers, and special characters.
3. Access Control: Access to information systems and data must be granted on a need-to-know basis. All personnel must have the minimum access necessary to perform their job duties.
4. Incident Response Plan: The organization must have an incident response plan that outlines the procedures to be followed in the event of a security incident. All personnel must be aware of their roles and responsibilities in the event of a security incident.
5. Regular Security Audits: The organization must conduct regular security audits to assess the effectiveness of its cybersecurity policies and procedures. Personnel must cooperate with the security audit team and provide any requested information or assistance.

Enforcement:

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. The organization reserves the right to take legal action against any individual who intentionally violates this policy and causes harm to the organization.

Conclusion:

Cybersecurity awareness and training is essential to protecting the organization's information systems, networks, and data. All personnel have a responsibility to comply with this policy and follow best practices to mitigate cybersecurity risks.