**End User Cyber Security Policies**

**Introduction**

End user cyber security policies establish the guidelines and requirements for individuals accessing and using digital systems or networks to ensure compliance with US law.

**Acceptable Use**

The policies define acceptable use of digital systems, outlining the activities that end users are permitted or prohibited from engaging in.

**Password and Account Security**

The policies emphasize the importance of strong passwords, regular password updates, and safeguarding of user accounts to protect against unauthorized access.

**Data Protection**

The policies address the protection of sensitive data, such as personally identifiable information (PII), and provide guidelines for secure storage, transmission, and disposal of data.

**Malware Prevention**

The policies outline measures to prevent malware infections, including regular software updates, use of reputable antivirus software, and exercising caution while opening email attachments or visiting unknown websites.

**Reporting Security Incidents**

The policies instruct end users on the procedures for reporting security incidents, including suspected breaches or unauthorized access, to enable swift response and mitigation.

**Mobile Device Security**

The policies address the security considerations for mobile devices, including the use of passcodes, encryption, and best practices for connecting to public Wi-Fi networks.

**Remote Work and Telecommuting**

If applicable, the policies provide guidelines for maintaining cyber security while working remotely, including the use of secure networks, VPNs, and adherence to organizational policies.

**Social Engineering and Phishing Awareness**

The policies educate end users about the risks of social engineering attacks and phishing attempts, encouraging vigilance and the reporting of suspicious activities.

**Compliance with Laws and Regulations**

The policies highlight the importance of adhering to relevant laws, regulations, and industry-specific requirements pertaining to cyber security, such as data privacy laws and industry compliance standards.

**Training and Awareness**

The policies may outline the requirement for regular cyber security training and awareness programs to educate end users about current threats, best practices, and their roles in maintaining a secure digital environment.

**Enforcement and Consequences**

The policies inform end users about the potential consequences for non-compliance with the cyber security policies, which may include disciplinary actions or legal consequences in accordance with US law.

**Updates and Modifications**

The policies clarify the process for updates or modifications to the cyber security policies, ensuring that end users are informed of any changes and required to comply with the updated policies.

**Contact Information**

The policies provide contact information for reporting cyber security concerns, seeking assistance, or obtaining additional information related to the policies.