Cyber Security Policy Creation Template

Document History

VERSION NUMBER	IMPLEMENTED BY	REVISION DATE	APPROVED BY	APPROVAL DATE	DESCRIPTION OF CHANGE

TABLE OF CONTENTS

1. INTRODUCTION

{This Template is designed for the creation of an effective Cyber Security Plan which captures the details of a Security risk in accordance with ISO/IEC 27001 – Information System Security}

2. SCOPE

{The Cyber Security Policy should include guidelines and provisions to mitigate security risks}

3. RESPONSIBILITY

{This policy applies to all company employees, contractors, volunteers, and anyone who has permanent, or temporary access to company systems, software, and hardware}

4. CYBER SECURITY BEST PRACTICE

{The Cyber Security policy should include details guidelines on the following:}

a. Enabling Firewall Protection
b. Updating Security Software
c. Enforcing Strong and safe Passwords
d. Using multi-factor authentication
e. Implementing regular Data Backups
f. Create a Cyber Security check list
g. Monitoring Third Party Controls

5. CONFIDENTIAL AND PROPRIETARY INFORMATION

{All confidential/Proprietary data should be identified and only accessible to authorized personnel} Data may include the following:

a. Unpublished financial information
b. Proprietary data on customer/partners/vendors
c. Any data pertaining to patents, infrastructure, or new technology
d. IT equipment, type, and usage
e. Software/Application License
f. Employee Information

6. COMPANY DEVICES SECURITY AND PROTECTION

{This policy should include guidelines for securing company-issued computers, tablets, cell phones, etc.} Policy should include guidelines for the following}

a. How to keep all passwords protected
b. Updated system, internet, and application security patches
c. Instructions on accessing systems via secure and private networks
d. Maintaining user accounts, passwords, and access privileges
e. Updating new user on-boarding packages

7. EMAIL SECURITY

{The Cyber Security plan should include guidelines for the safekeeping and monitoring of email accounts to avoid scams, and malicious software.

8. DATA SECURITY

{The Cyber Security policy should include guidelines for the proper use of data to maintain adequate and effective data security}

9. DATA TRANSFERS

{Data Transfers can introduce critical risks to company systems. The Cyber security policy should include guidelines for the following:}

a. How to avoid transferring un-encrypted sensitive data to other devices or accounts.
b. How to share confidential data over company networks/system and not a public WI-FI or private networks
c. How to ensure that the recipients/organization are authorized with adequate security policies
d. How to report scams, privacy breaches and hacking attempts.

10. SECURITY AGREEMENTS

{The Cyber Security Policy should include a list of security agreement between organizations, both internal and external}

11. SYSTEM BACKUP POLICY

{The Cyber Security Policy should include guidelines to meet the company's' business objective and ensure continuity of operations. It should include information/instructions on the following}

a. Type of Backup Media
b. Type of backups performed; Full, Incremental, Partial, Restoration
c. Scheduled dates, Times, and storage locations

12. ACCEPTABLE USE INFORMATION

{The Acceptable Use section governs the use and security of all information and computer equipment, including the proper use of email, internet, voice and computing equipment}

13. SOCIAL MEDIA USAGE

{The Cyber Security Policy should include guidelines for the proper use of social media for product promotions and interacting with external customers/vendors. The policy should cover all Social Media platforms including Facebook, Instagram, LinkedIn, Twitter, Google+, Wikipedia, and other social networking sites}

14. CYBER SECURITY RISKS

{Include guidelines to Identify potential risks and plans for mitigation}

15. CYBER SECURITY RISK ASSESSMENTS

{Include guidelines which examines the organization's IT infrastructure to control and remediate vulnerabilities}.

16. VOLUNERABILITY MANAGEMENT

{Include guidelines for a systematic review of security weaknesses in the information system.

17. INCIDENT REPORTING

{The Cyber Security policy should include guideline to capture the details of an incident, such as a click on a phishing link, when it happens or shortly after.