tyler cybersecurity™

SAMPLE

Information Security / Cybersecurity Program

This document is the confidential property of ORGANIZATION.

Any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission from ORGANIZATION is strictly prohibited.

tyler technologies

One Tyler Drive
Yarmouth, ME 04096
800.772.2260

Purpose

The following Sample Information Security / Cybersecurity Program outlines the components of a comprehensive information security / cybersecurity program. Each section includes a description, as well as what the corresponding policy should include. Organizations may use this document as a starting point for building a comprehensive program or as a reference to enhance an existing program.

Introduction

Cybersecurity isn't a destination, it's a sustainable Program of interdependent processes and controls. The world of cybersecurity is dynamic, so you need to be able to prepare for and adapt to changing conditions in order to withstand and recover rapidly from disruptions.

An effective Information Security / Cybersecurity Program requires a strategic approach, and an Information Security / Cybersecurity Policy is the foundation for success. A solid policy is built with straightforward rules, standards, and agreements that conform to industry best practices and regulatory requirements. It provides institutional memory that survives inevitable changes in personnel. It clearly defines information security expectations, activities, roles, and responsibilities. Its requirements, values, and goals must also reflect those of the organization's culture as a whole.

SAMPLE

Information Security / Cybersecurity Policy Objectives

The objective of an Information Security / Cybersecurity Policy and corresponding program is to:

1. Protect the organization, its employees, its customers, and also vendors and partners from harm resulting from intentional or accidental damage, misuse, or disclosure of information;
2. Protect the integrity of the information; and
3. Ensure the availability of information systems.

Seven Characteristics of a Successful Information Security / Cybersecurity Policy

Successful Information Security / Cybersecurity Policies establish what must be done and why it must be done, but not how to do it. Good policy has the following seven characteristics, each equally important:

1. Endorsed – The policy has the support of management.
2. Relevant - The policy is applicable to the organization.
3. Realistic – The policy makes sense.
4. Attainable – The policy can be successfully implemented.
5. Adaptable – The policy can accommodate change.
6. Enforceable – The policy is statutory.
7. Inclusive – The policy scope includes all relevant parties.

Table of Contents

1. Information Security Program Governance 4
2. Information Security Program Maintenance & Review 4
3. Information Security Risk Management 5
4. Information Classification & Management 5
5. Incident Management 6
6. Access Control 6
7. Infrastructure Security 6
8. Operational Security 7
9. System Lifecycle Security 7
10. Physical & Environmental Security 8
11. Contingency Planning 8
12. Personnel Security 8
13. Third-Party Management & Oversight 9
14. Electronic Banking / Online Payment Security 9
15. Social Media 9
16. Compliance 10
Appendix A: GLBA / HIPAA Information Security Policy Cross Reference 11
About Tyler Cybersecurity 12

SAMPLE

1. Information Security Program Governance

A successful Information Security Program requires oversight and management.

Goals & Objectives: (include goals and objectives of your Information Security Program Governance Policy)

Information Security Program Governance Policy

Your Information Security Program Governance should address the following roles:

1.1. Board of Directors
1.2. Risk Management Committee
1.3. Senior Management
1.4. Information Security Officer (ISO).
1.5. Information Security Committee (ISC)
1.6. Compliance Officer
1.7. Physical Security Officer
1.8. Internal Audit
1.9. Incident Response Team (IRT)
1.10. Information Technology Management and Staff
1.11. Information Owners
1.12. Employees

List Relevant Documents:

SAMPLE

2. Information Security Program Maintenance & Review

Information Security is an evolving process that changes based upon the dynamic nature of risks, threats, vulnerabilities, and the information systems themselves. In order to maintain a secure posture, it is essential that the Information Security Program be thought of as a "living document" that responds to the changing environment through its operational practice and a consistently applied process of maintenance and review.

Goals & Objectives: (include goals and objectives of your Information Security Program Maintenance & Review Policy)

Information Security Program Maintenance & Review Policy

2.1. Compliance
2.2. Information Security Policy
2.3. Documentation
2.4. Program / Policy Review
2.5. Internal Audits
2.6. Self-Assessments
2.7. Independent Review
2.8. Information Security Expertise

List Relevant Documents:

3. Information Security Risk Management

ORGANIZATION identifies, measures, monitors, and controls information security related risks, including those relating to cybersecurity.

Goals & Objectives: (include goals and objectives of your Information Security Risk Management Policy)

Information Security Risk Management Policy

3.1. Risk Management
3.2. Risk Assessment
3.3. ORGANIZATION Board of Directors
3.4. Risk Management Committee
3.5. Information Security Committee
3.6. Chief Information Officer (CIO)
3.7. Chief Risk Officer (CRO)
3.8. Internal Auditor
3.9. Physical Security Officer
3.10. Compliance Officer
3.11. Department Managers
3.12. Legal Counsel of ORGANIZATION
3.13. Employees
3.14. Audit

List Relevant Documents:

SAMPLE

4. Information Classification & Management

ORGANIZATION requires that all business units of ORGANIZATION establish appropriate procedures, systems and practices to maintain records in accordance with applicable regulations and ORGANIZATION's defined business needs.

Goals & Objectives: (include goals and objectives of your Information Security Classification & Management Policy)

Information Security Classification & Management Policy

4.1. Information Classification
4.2. Information Ownership
4.3. Distribution / Dissemination of Protected or Confidential Information
4.4. Retention
4.5. Destruction of Protected or Confidential Information
4.6. Coordination with Business Continuity Planning

List Relevant Documents:

5. Incident Management

An Incident Response plan must be created, documented, communicated and tested to ensure all ORGANIZATION's personnel understand how to identify and respond to security incidents.

Goals & Objectives: (include goals and objectives of your Incident Management Policy)

Incident Management Policy

5.1. Incident Response
5.2. Unauthorized Access to Customer Accounts / Patient Information

List Relevant Documents:

6. Access Control

Access Control is the process of assuring that properly approved users are granted appropriate access to information and/or information systems.

Goals & Objectives: (include goals and objectives of your Access Control Policy)

SAMPLE

Access Control Policy

6.1. User Access
6.2. Administrator / Privileged Account Access
6.3. User Provisioning
6.4. Termination of Access
6.5. Identification and Authentication
6.6. Passwords
6.7. Logon Parameters
6.8. Sessions
6.9. Access Review

List Relevant Documents:

7. Infrastructure Security

Information Security-related controls and best practices are integrated into the network design, architecture, and operation.

Goals & Objectives: (include goals and objectives of your Information Security Classification & Management Policy)

Information Security Classification & Management Policy

7.1. Network Access
7.2. Network Architecture
7.3. Wireless Networks
7.4. Border Protection (Intrusion Detection / Prevention & Firewall)
7.5. VPN Remote Access
7.6. Modem Use

7.7. Servers and Workstations
7.8. Mobile Devices (Laptops, Smartphones, Tablets)
7.9. Internet Access
7.10. Content Filtering / Monitoring
7.11. Email

List Relevant Documents:

8. Operational Security

Operational Security controls address information security in the context of daily ORGANIZATION operations.

Goals & Objectives: (include goals and objectives of your Operational Security Policy)

Operational Security Policy

8.1. Change Management
8.2. Implementation of Vendor-Supplied Changes
8.3. Change Documentation
8.4. Anti-virus Management & Malicious Code
8.5. Patch Management
8.6. Dual Controls
8.7. Encryption
8.8. Activity Review

List Relevant Documents:

SAMPLE

9. System Lifecycle Security

Information Security is engrained in the Lifecycle of Information Systems at ORGANIZATION from the acquisition process to disposal.

Goals & Objectives: (include goals and objectives of your System Lifecycle Security Policy)

System Lifecycle Security Policy

9.1. Acquisition
9.2. Development
9.3. Software Licensing
9.4. Inventory
9.5. Security Baselines
9.6. Pre-Production Testing & Approval
9.7. Operating Environments
9.8. System Documentation
9.9. System Retirement

List Relevant Documents:

10. Physical & Environmental Security

This section represents the intersection of the Information Security Program with traditional security controls for protecting against physical damage, destruction and theft of Information Systems and data.

Goals & Objectives: (include goals and objectives of your Physical & Environmental Security Policy)

Physical & Environmental Security Policy

10.1. Organizational Policy
10.2. Responsibilities and Reporting
10.3. Physical Security Controls
10.4. Identification
10.5. Operations Center Security
10.6. Data Center Controls
10.7. Branch Controls
10.8. Media Storage

List Relevant Documents:

SAMPLE

11. Contingency Planning

Contingency Planning prepares ORGANIZATION for continuity of operations under adverse operating conditions. Continuity describes the capability to sustain operations through unforeseen and/or unexpected events.

Goals & Objectives: (include goals and objectives of your Contingency Planning Policy)

Contingency Planning Policy

11.1. Business Impact Analysis
11.2. Data Archiving
11.3. Disaster Recovery Planning
11.4. Pandemic Planning

List Relevant Documents:

12. Personnel Security

Information security controls and best practices extend to all potential and current employees. Every person who performs work for or has access to ORGANIZATION has certain roles, responsibilities, and accountability for helping to ensure the confidentiality, integrity, accessibility, and security of ORGANIZATION data.

Goals & Objectives: (include goals and objectives of your Personnel Security Policy)

Personnel Security Policy

12.1. Organization Policy
12.2. Background Screening
12.3. Information Systems Acceptable Use Policy
12.4. Clean Desk / Clean Screen / Office Etiquette

12.5. Expectation of Privacy
12.6. Security Awareness and Training

List Relevant Documents:

13. Third-Party Management & Oversight

Third-parties are required to comply with applicable security procedures, policies, and regulations that ORGANIZATION has designed its security program to comply with.

Goals & Objectives: (include goals and objectives of your Third-Party Management and Oversight Policy)

Third-Party Management and Oversight Policy

13.1. Organizational Policy
13.2. New Vendors and Contractual Relationships
13.3. Due Diligence
13.4. Contract Language
13.5. Proof of Insurance
13.6. Monitoring
13.7. Third-Party Access

List Relevant Documents:

SAMPLE

14. Electronic Banking / Online Payment Security

Electronic Banking / Online Payment Security controls have been implemented to reduce the risk and exposure.

Goals & Objectives: (include goals and objectives of your Electronic Banking Security Policy)

Electronic Banking Security Policy

14.1. Risk Management
14.2. Authentication
14.3. Administrative Access
14.4. Member Enrollment, Setup and Maintenance
14.5. Monitoring Electronic Banking Activity
14.6. Linking to Third-Party Services / Sites
14.7. Detecting / Preventing Fraud
14.8. Cryptographic Controls
14.9. Disaster Recovery & Business Continuity

List Relevant Documents:

15. Social Media

Social Media applications introduce the need to carefully control their configuration and use to ensure the benefits are realized and the risks are minimized.

Goals & Objectives: (include goals and objectives of your Social Media Policy)

Social Media Policy

15.1. Organizational Policy
15.2. Social Media Application Standards
15.3. Incident Response Procedures

List Relevant Documents:

16. Compliance

This policy outlines the duties and responsibilities regarding the implementation of a compliance program to ensure that all employees of ORGANIZATION are knowledgeable and consistent in their application of laws.

Goals & Objectives: (include goals and objectives of your Compliance Policy)

Compliance Policy

16.1. Organizational Policy
16.2. Board of Directors
16.3. Compliance Officer
16.4. Supervisory Committee
16.5. Other Roles and Responsibilities

List Relevant Documents:

SAMPLE

Appendix A: GLBA / HIPAA Information Security Policy Cross Reference

If you are a financial institution or healthcare organization (covered entity), this is where you would cross reference your Information Security policies to GLBA / HIPAA requirements.

SAMPLE

About Tyler Cybersecurity

The Tyler Cybersecurity team has worked with clients to develop effective cybersecurity programs and policies for almost two decades. Our methodology is collaborative and nature. Together, we assess your existing security practices, and determine whether they comply with pertinent regulatory requirements and/or legal standards and align with best practices. Then we expand and build on them strategically to create a comprehensive Information Security Policy tailored to specific business objectives and cybersecurity maturity goals.

Founded in 2002, we were acquired by Tyler Technologies, Inc. in 2018. We offer a suite of services to support your entire cybersecurity lifecycle, including program development, education and training, tech testing, advisory services, and digital forensics. Complementing our services is Tyler Detect Managed Threat Detection that delivers advanced threat detection, incident response support, and compliance reporting across your entire environment, including end points, all without the need to invest in costly hardware devices or dedicated resources. Partner with Tyler to ensure your organization is fully trained, compliant, and prepared for evolving cybersecurity threats. Learn more at www.tylercybersecurity.com.

Tyler Technologies (NYSE: TYL) provides software and services to transform communities. Tyler's solutions connect data and processes across disparate systems, allowing clients to gain actionable insights for solving problems. Tyler has more than 21,000 successful installations across 10,000 sites, with clients in all 50 states, Canada, the Caribbean, Australia, and other international locations. A financially strong company, Tyler has achieved double-digit revenue growth every quarter since 2012. It was also named to Forbes' "Best Midsize Employers" list in 2018 and recognized twice on its "Most Innovative Growth Companies" list. More information about Tyler Technologies, headquartered in Plano, Texas, can be found at tylertech.com.

SAMPLE