SOTI

ONE PLATFORM - CONNECTING EVERYTHING

SECURITY POLICY ESSENTIALS

SOTI security policies address the controls in the ISO 27001/27002 standard. The following are the security policy essentials:

Vulnerability Management Policy:

Establishes guidelines to reduce the security risk associated with technical systems vulnerabilities and software installed by users. It also outlines anti-virus and malware protection, as well as Windows Security settings.

Information Security Policy:

Establishes guidelines to reduce the security risk associated with information asset and resource management. It also outlines the Information Security Management System (ISMS) and provides many policy statement details from sanctions to risk, logs, network, and cryptography management.

Access Control Policy:

Establishes guidelines to reduce the security risk associated with user identity authentication, systems and development access control, and privileged access rights management.

Device Policy:

Establishes guidelines to reduce the security risk associated with the use of device assets, as well as protocols for dealing with that usage.

Information Technology Resource Usage Policy:

Establishes guidelines for using company resources, included email and the Internet. This applies to employee conduct and accountability with these resources, including (but not limited to) those policies dealing with intellectual property protection, privacy, misuse of company resources, information and data security, and confidentiality.

Security Incident Management Policy:

Establishes guidelines to reduce the security risk associated with incidents. It also details phases of the incident life cycle and the management of actions taken to resolve incidents.

Supplier Management Policy:

Establishes guidelines to reduce the security risk associated with outsourcing and the use of suppliers.

Inventory and Asset Classification Policy:

Establishes guidelines to reduce the security risk associated with the handling and protection of information assets (including removable media and equipment). It also details information asset inventory and classification.

Systems Development Lifecycle Policy:

Establishes guidelines to reduce the security risk associated with the acquisition, development, and maintenance of information systems. It also outlines security risks management, software and systems development/testing, and quality assurance activities.

Cloud Development Lifecycle Policy:

Establishes guidelines to reduce the security risk associated with an information system. It also establishes processes for planning, creating, testing, and deploying that system.

ISMS Audit and Compliance Policy:

Establishes guidelines to reduce the security risk associated with Information Security Management System controls and non-conformity management. It also establishes independent review of related policies and technical compliance.

Change Management Policy:

Establishes guidelines to reduce the security risk associated with changes to network, systems, and other information assets.

SOTI is a proven innovator and industry leader for simplifying business mobility and IoT solutions by making them smarter, faster and more reliable. SOTI helps businesses around the world take mobility to endless possibilities.

soti.net

Copyright © 2018 SOTI Inc. All rights reserved.