**DATA SECURITY PLAN TEMPLATE**

| VERSION HISTORY |
| --- |
| VERSION | APPROVED BY | REVISION DATE | DESCRIPTION OF CHANGE | AUTHOR |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

DATA SECURITY PLAN

COMPANY NAME

Street Address

City, State and Zip

webaddress.com

Version 0.0.0

00/00/0000

1. **SYSTEM IDENTIFICATION**

Details on system, system owner, number of users

1. **SYSTEM ENVIRONMENT**

Details on system interconnections, key devices, hardware and software components

1. **REQUIREMENTS**

Details on any data security requirements that are applicable

* 1. **Access Control**

Ensure system limits access to authorized users, sets type of transactions allowed, limits certain functions to "privileged" users, monitors remote access, controls connection of mobile devices

* 1. **Awareness and Training**

Ensure everyone in organization is aware of system security risks, are adequately trained to perform activities in a way that protects data, understand indicators of threats or infiltrations

* 1. **Audit and Accountability**

Ensure organization has an ongoing system that monitors any unusual or unauthorized activity in the system

* 1. **Configuration Management**

Establish and maintain baseline configurations throughout the system, including controlling and monitoring user-installed software

* 1. **Identification and Authentication**

Ensure system can identify system users and devices, enforce a minimum password complexity

* 1. **Incident Response**

Establish system that tracks, documents and reports incidents that may have compromised security and tests the organizations ability to respond to an incident

* 1. **Maintenance**

Perform continual maintenance to the system

* 1. **Media Protection**

Limit access to the system's digital media to authorized users and ensure the digital media is kept safe in other ways

* 1. **Personnel Security**

Screen people before allowing access to system and ensure the system is protected after people leave the organization

* 1. **Physical Protection**

Limit access to the physical systems and equipment to authorized people

* 1. **Risk Assessment**

Periodically assess the security risks in the normal operation of the system, and scan for vulnerabilities and make fixes when vulnerabilities are found

* 1. **Security Assessment**

Periodically assess the security controls to ensure they are effective and make fixes where necessary

* 1. **System and Communications Protection**

Monitor and protect communications from outside the system that are received by the system

* 1. **System and Information Integrity**

Identify, report and correct system flaws in a timely manner, provide protection from malicious code and monitory security alerts and advisories

|  |
| --- |
| **DISCLAIMER**Any articles, templates, or information provided by Smartsheet on the website are for reference only. While we strive to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, articles, templates, or related graphics contained on the website. Any reliance you place on such information is therefore strictly at your own risk. |