August 19, 2021

Risk Assessment Report

Your Company

123 Fake Street
Faux City, NX 99999

555-555-5555

ATTN:

**Summary**

On Mission IT, is pleased to offer our Risk Assessment for your inspection. Risk Assessments are part of ensuring regulatory compliance with security policies. Our approach is to identify these risk factors and provide remediation actions in a proactive approach to building and maintaining a regulatory compliant organization.

**Proposed Actions**

The goal of this Risk Assessment is to identify risk factors that could lead to a data breach and help your practice to become compliant with all regulatory components. In this audit, we assess the effectiveness of the technical and administrative safeguards used to protect sensitive personal data. The risks that we have identified are listed below, with the actions required to remediate these compliance issues.

**Analysis**

A complete breakdown of the risks we have discovered and the remediation actions required to bring it to into compliance.

|  **Risk**  |  |  |  **Remediation** |
| --- | --- | --- | --- |
| Inventory Not Performed or Updated –conduct a yearly inventory of all devices that access sensitive information |  | To resolve this issue, an inventory must be:* Conducted annually and kept with risk assessment materials
* Include desktops, laptops, tablets, and mobile devices
* Note device name, serial number, OS version, and update status
* Note employee assignment, device location, and encryption status
 |
| User Computer Operating System Out of Compliance—the operating system for all user devices must be currently supported by the manufacture to receive security updates |  | Required actions to resolve this risk are:* Remove any defunct operating system from the network
* Update the operating system to a currently supported version
* Pay for extended service on the old operating system to receive security updates (if available)
* Replace the device
 |
| Insufficient Server Maintenance—not performing updates in a timely fashion on servers can allow software vulnerabilities to be remotely exploited |  | * Contract with an IT Support company to perform computer maintenance **-or-**
* Implement a Network Security Update Policy to ensure that all servers are updated within 90 days of patch release
 |
| Lack of Policies and Procedures—formal policies and procedures are needed to communicate security expectations |  | Maintain and update a security-based omnibus that is made available to all workforce members and contains:* Administrative security policies
* Technical security policies
* Physical security policies
* Hardware Inventory
* Software Inventory
* 6 years of risk assessments
* Corrective action plans related to the risk assessments
 |
| Policies and Procedures Not Reviewed or Updated—review and update policies and procedures in response to security needs and changes in business practices  |  | The Privacy Officer and members of Management/Ownership periodically perform a formal review of policies and procedures to:* Ensure employee consistency
* Address business changes
* Address security changes
 |
| No Security Official Identified—document a point of contact for making employees aware of security issues |  | Implement a Security Awareness program with a Security Officer to focus on administrative, physical, and technical safeguards, including:* Develop, enforce, assess, and amend policies and procedures
* Appoint a Compliance Officer.
* Conduct internal monitoring and auditing
* Respond to breaches and take corrective action
 |
| Policy Updates—existing policies may not address the current security requirements to maintain all administrative, technical, and physical security standards |  | Review all policies to ensure they conform to current security standards |

If your organization deals with Personally Identifiable Information (PII) or electronic Protected Health Information (ePHI), we can provide you with all the information to ensure that you are fully compliant with the appropriate regulatory requirements, including all Technical, Physical, and Administrative Safeguards, Breach Notification Rules, the updated Omnibus, Enforcement Rules, and more.