YourIT!
Your Logo Goes Here

NIST CSF Assessment

NIST CSF Protect Worksheet

Prepared for:
Your Client's Company
Prepared by:
YourIT Company

Table of Contents

Identity Management, Authentication and Access Control (PR.AC)

1.1 - Identity and Credential Management

Does the organization have a documented process to issue, manage, verify, revoke and audit identities and credentials? Attach the relevant policies and procedures or other documentation.

No

1.2 - Physical Access

Is physical access to assets managed and protected? Attach photo evidence of locks, cameras and security measures. If no, please note any deficiencies in the notes.

No

1.3 - Remote Access

Is remote access managed?

No

1.4 - Network Segregation and Segmentation

Is network segregation or network segmentation employed as a means to protect network integrity?

No

1.5 - Application and System Access

List any applications (on-premise or SaaS) and note if authentication is required.

Application	Is Authentication Required
Sales Force	Yes
etrigue	No
Office365	Yes
Happy Fox	Yes

1.6 - Asset Authentication

In reviewing the authentication methods used for users, devices, and other assets, were any deficiencies found where the method of authentication (e.g., single-factor, multi-factor) not commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)?

No

Awareness and Training (PR.AT)

2.1 - All Users

Do all users receive cybersecurity awareness education and training as part of their on-boarding and on a routine basis? Please note or attach any logs or reference to training materials used.

No

2.2 - Privileged Users

Do privileged users receive enhanced cybersecurity awareness education and training describing their roles and responsibilities? Please note or attach any logs or reference to training materials used.

No

2.3 - Third-party Stakeholders

Do you communicate to third-party stakeholders their roles and responsibilities with regards to cybersecurity? Please note or attach any logs or reference to training materials used.

No

2.4 - Senior Executives

Do senior executives receive enhanced cybersecurity awareness education and training describing their roles and responsibilities? Please note or attach any logs or reference to training materials used.

No

2.5 - Physical and Cybersecurity Personnel

Do physical and cybersecurity personnel receive enhanced cybersecurity awareness education and training describing their roles and responsibilities? Please note or attach any logs or reference to training materials used.

No

Data Security (PR.DS)

3.1 - Data-at-rest

Do your organization protect data-at-rest?

No

3.2 - Data-in-transit

Do your organization protect data-in-transit?

No

3.3 - Asset Removal, Transfers, and Disposition

Do your organization formally manage assets throughout removal, transfers, and disposition?

No

3.4 - Data Capacity

Does your organization employ a monitoring system to ensure adequate disk and storage is available to ensure data availability?

No

3.5 - Protection Against Data Leaks

Does your organization deploy firewalls between the internal network and all externally facing network connections?

No

3.6 - Software, Firmware, and Information Integrity

Does your organization employ integrity checking mechanisms are used to verify software, firmware, and information integrity?

No

3.7 - Separation of Development/Testing from Production Environments

Is the development and testing environment(s) separated from the production environment? If yes, please attach a network diagram depicting components of the development/testing environment and production environment.

No

3.8 - Hardware Integrity

Does your organization employ integrity checking mechanisms are used to verify hardware integrity?

No

Information Protection Processes and Procedures (PR.IP)

4.1 - Information Technology/Industrial Control Systems

Has your organization created and maintains a baseline configuration of information technology/industrial control systems incorporating security principles (e.g. concept of least functionality)? Attach any supporting documents.

No

4.2 - System Development Life Cycle

Has your organization implemented a System Development Life Cycle to manage systems? Attach any supporting documents.

No

4.3 - Configuration Change Control Processes

Does your organization have configuration change control processes are in place? Attach any supporting documents.

No

4.4 - Information Backups

Are backups of information are conducted, maintained, and tested? Attach any supporting documents.

No

4.5 - Physical Operating Environment

Are policy and regulations regarding the physical operating environment for organizational assets met? Attach any supporting documents.

No

4.6 - Data Destruction

Is data is destroyed according to policy? Attach any supporting documents.

No

4.7 - Protection Process Improvement

Are protection processes regularly reviewed and improved? Attach any supporting documents.

No

4.8 - Protection Technology Effectiveness

Is the effectiveness of protection technologies is shared? Attach any supporting documents.

No

4.9 - Response and Recovery Plans

Are response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) in place and managed? Attach any supporting documents.

No

4.10 - Response and Recovery Plan Testing

Are response and recovery plans regularly tested? Attach any supporting documents.

No

4.11 - Human Resources Practices

Is Cybersecurity included in human resources practices (e.g., deprovisioning, personnel screening)? Attach any supporting documents.

No

4.12 - Vulnerability Management Plan

Has a vulnerability management plan been developed and implemented? Attach any supporting documents.

No

Maintenance (PR.MA)

5.1 - Maintenance and Repair of Organizational Assets

Are maintenance and repair of organizational assets performed and logged, with approved and controlled tools? Attach any supporting documents.

No

5.2 - Remote Maintenance of Organizational Assets

Is remote maintenance of organizational assets approved, logged, and performed in a manner that prevents unauthorized access? Attach any supporting documents.

No

Protective Technology (PR.PT)

6.1 - Audit/log Records

Are audit/log records determined, documented, implemented, and reviewed in accordance with policy? Attach a copy of the relevant Policy and Procedures.

No

6.2 - Removable Media

Is removable media is protected and its use restricted according to policy? Attach a copy of the relevant Policy and Procedures.

No

6.3 - Principle of Least Functionality

Is the principle of least functionality incorporated by configuring systems to provide only essential capabilities?

No

6.4 - Communication and Control Networks

Are communications and control networks protected?

No

6.5 - Resilience Requirements

Are mechanisms (e.g., failsafe, load balancing, hot swap) implemented to achieve resilience requirements in normal and adverse situations? Please note the type of mechanisms.

No