[Org Name]

Security Assessment Report

Version 1 - [Date]

The following confidential document describes the initial assessment of digital security practices at [ORGANIZATION] as suggested by Access Now Digital Security Helpline. Within this document we present a brief background describing the current situation, followed by identified challenges and a proposed remediation plan.

Background

[Background context of organization] - see instructions in README.

Identified Challenges

During an initial assessment performed by the Access Now Digital Security Helpline and tracked as [accessnow [$CASE NUMBER]], the following digital security challenges and opportunities were identified:

[what follows is a list of examples, please use the ones that apply or add new ones to your report]

- Securing internal and external communications
- Improving access controls for social media accounts
- Updating security policy, including policies on backups and travel
- Adopting best practices for password usage and management
- Strengthening website security practices
- Updating operating systems across the organization
- Training staff on best security practices
- Protecting the organization's computers and systems from

hacking by politically motivated external actors
- Developing a strategy to limit the damage in case one of the organization's devices is lost or stolen
- Reducing the risk of leaks
- Securing storage
- Securing email accounts
- Securing social media accounts
- Working on DDOS protection on the website
- Strengthening physical security

Remediation Plan

In order to address the challenges presented above, the Helpline is available to assist [$ORGANIZATION] with the design, prioritization, and implementation of a remediation plan. There may also be other implementing partners whom [$ORGANIZATION] would like assistance from instead.

We recommend [$ORGANIZATION] IT staff lead the implementation of the remediation plan, and ensure they have adequate buy-in and support from the rest of the organization to implement these new organizational practices.

If the plan is accepted, the Helpline will create dedicated threads with [$ORGANIZATION] staff for each remediation topic and include associated information to support implementation.

[What follows is a list of examples. Please use the ones that apply, edit the descriptions, and/or add new items to your report. Items could have different priorities than in the examples, and based on the results of the assessment may be assigned a higher or lower priority.]

High Priority Tasks

Ensure all operating systems are supported

Some of the organization devices, are running potentially unsupported operating systems such as [unsupported OS name]. Ensuring that all devices are running up-to-date and supported operating systems will greatly improve the ability of the organization to protect information and assets. As a registered charity, [$ORGANIZATION] may be able to use TechSoup for discount

purchases of Microsoft products.

Ensure previously infected workstations are cleaned or replaced

Collect more information about the remediation steps that occurred for workstations that had previously been infected, in order to ensure that they have been adequately cleaned or replaced.

Secure communications with sources

Explore whether it is possible to suggest safer communications platforms for sources.

Improve Access Controls

Important staff communications services and platforms such as email, chat, file sharing, and project management should be configured with access controls such as multi-factor authentication wherever possible.

Ensure Unique and Strong Passwords

Passwords used for accessing the organization's computers and online accounts (email, chat, social networks, file sharing, etc.) should be unique and strong, i.e. consisting of at least 20 characters and containing lower- and upper-case letters, numbers and symbols. Password managers are encouraged to easily manage these passwords.

Set up staff with password managers

All staff should use password managers in order to create and maintain strong passwords for their accounts. This could be a local password manager such as KeePassXC, or we can work with the organization to identify a secure workflow for sharing passwords among the team.

Configure SSL/TLS on organization website

Set SSL/TLS on the website [website URL] to protect the visitors' privacy. We can either explore the options provided by the host provider or, if possible, use a free Let's Encrypt certificate.

Full Disk Encryption of All Hard Drives and Storage Devices

All computers containing sensitive materials and communications should be protected with full-disk encryption. This also includes USBs, hard drives, and other external media containing sensitive or confidential information.

Cloud Storage Account Security

Given [$ORGANIZATION]'s reliance on cloud storage for organizational data, securing access to these accounts is an important step. This implies enabling two-factor authentication and securing access to the email accounts associated with the storage accounts.

Medium Priority Tasks

Secure internal communication workflows

Explore secure communications platforms or tools such as [tool names] to better enable the team to communicate confidentially with each other and partners.

Move sensitive workflows to Qubes OS

Exploring moving workflows used for highly sensitive communications and information sharing to Qubes OS, in order to improve usability and security. The helpline can provide assistance in hardware acquisition, setup, training, and troubleshooting.

Organizational security policies

Capture existing practices and incorporate updated workflows for different services and tools used by staff into the organization's policies, and have those policies readily accessible by staff members for reference.

Backup policy

A backup policy is recommended to recover from any data loss. Based on the operating systems used by the staff and the distribution of data across the organization's devices and servers, the policy needs to address how data is backed up and include a restoration plan.

Travel policy

Given staff travels frequently, we recommend that the organization

captures their existing practices into a travel policy. We can work with the organization to define the best practices for the staff while crossing the [country] borders based on the laws and known practices in the country.

Basic Digital Security Hygiene

Ensure that common staff communications such as email and chat are done in a more secure manner and that the organizational security policies are implemented by all staff.

Conduct a Security Audit

Hire a professional to conduct a security audit aimed at identifying and documenting asset vulnerabilities, as well as internal and external threats; acquiring threat and vulnerability information from external sources; identifying potential business impacts and likelihoods; determining enterprise risk by reviewing threats, vulnerabilities, likelihoods, and impacts.

Create a Data Breach Plan

Create a plan to address a prospective data breach, aimed at containing the problem, securing [$ORGANIZATION]'s systems and channels of communication, and mitigating any damage that may have been caused by the breach.

Offboarding Policy

Create a policy to ensure that when a member of the team leaves the organization, necessary actions are taken around access to shared online resources as well as the secure wiping of the used devices.

Low Priority Tasks

Backup website

Explore the options available through the hosting provider to enable an onsite backup for the website, as well as methods to locally back up the website. This would help recover from incidents like website defacement or data loss.

DDoS Protection

In order to mitigate the threat of DDoS attacks on

[$ORGANIZATION]'s website, we recommend the adoption of a free DDoS protection service.

Improve Security Awareness

Work with [$ORGANIZATION] to identify strategies to perform digital security awareness exercises. This could include, for example, a security awareness talk, monthly digital security emails, security tip of the week, etc. Access Now could provide [$ORGANIZATION] with materials useful to complete this action item.

[$IH name]
Security Incident Handler | [$EMAIL]
For more information, please visit: accessnow.org/help
Access Now Helpline Terms of Service:accessnow.org/terms-of-service/
