**CYBERSECURITY TOOLKIT**

 **FOR**

**CIVIL SOCIETY ORGANIZATIONS**

February 2024

Table of Contents

[Introduction 4](#_Toc159655386)

[Cybersecurity Terminologies and Glossaries 5](#_Toc159655387)

[Cybersecurity Q&A for Civil Society Organizations 7](#_Toc159655388)

[Cybersecurity Awareness Resources 9](#_Toc159655389)

[Daily Digital Security Routine Checklist 11](#_Toc159655390)

[Essential Cybersecurity Training for Employees 12](#_Toc159655391)

[Secure Password Creation and Management Tools 14](#_Toc159655392)

[Email Security Best Practices Checklist 16](#_Toc159655393)

[Mobile Device Security Checklist 17](#_Toc159655394)

[Social Media Security Awareness Guide 18](#_Toc159655395)

[Cybersecurity for Remote Workers: A Guide 20](#_Toc159655396)

[Digital Hygiene Best Practices 23](#_Toc159655397)

[Cybersecurity Policy Template for Organizations 26](#_Toc159655398)

[Cybersecurity Template for Organizations 27](#_Toc159655399)

[Digital Security Policy Template for CSOs 30](#_Toc159655400)

[Digital Security Policy Template (Short Version) 36](#_Toc159655401)

[Data Protection Policy Template 38](#_Toc159655402)

[Incident Response Plan Template 39](#_Toc159655403)

[Security Risk Assessment Form 41](#_Toc159655404)

[Security Risk Assessment Form 44](#_Toc159655405)

[Network Security Checklist for Small Offices 46](#_Toc159655406)

[Digital Security Audit Checklist for CSOs 50](#_Toc159655407)

[Business Continuity Planning Template tailored for CSOs, focusing on digital security measures 52](#_Toc159655408)

[Template for Partner Collaboration Agreement Including Digital Security Expectations 53](#_Toc159655409)

[Digital Tools Usage Agreement for Staff and Volunteers 56](#_Toc159655410)

[Vulnerability Scanning and Reporting Checklist 58](#_Toc159655411)

[Directory of Digital Security Tools and Services 59](#_Toc159655412)

[Cybersecurity Awareness Posters: A Guide 61](#_Toc159655413)

[Data Encryption Techniques 63](#_Toc159655414)

[Digital Incident Report Form 66](#_Toc159655415)

[Template for Partner Collaboration Agreement Including Digital Security Expectations 67](#_Toc159655416)

[Social Media Security Protocols Guide for CSOs 68](#_Toc159655417)

[Email Security Checklist 70](#_Toc159655418)

[Quick Cybersecurity Checkup Checklist 72](#_Toc159655419)

[Resources 74](#_Toc159655420)

# **Introduction**

In today's digital world, cybersecurity is crucial for everyone, including civil society organizations (CSOs). These organizations play a key role in our communities, advocating for social change, providing essential services, and supporting vulnerable populations. However, cyber threats, such as data breaches, phishing attacks, and malware, can jeopardize their valuable work. Cybersecurity measures are about more than just protecting data; they safeguard the mission and trust of these organizations.

This toolkit aims to provide CSOs with a comprehensive resource to understand and improve their cybersecurity practices. We recognize that not everyone has a technical background, and the world of cybersecurity can seem overwhelming. That's why we've gathered various resources, from policy templates to practical checklists and user-friendly guides, all tailored for non-technical users. These resources cover different aspects of cybersecurity, such as creating strong passwords, securing remote work, and managing digital hygiene.

For this toolkit, **cybersecurity** encompasses all practices aimed at protecting our digital lives from cyberattacks, while **digital security** focuses specifically on safeguarding personal and organizational online information and identities. Together, they form a comprehensive approach to securing our digital world.

While some information may appear repeated across different sections, this repetition is intentional to emphasize the importance of certain cybersecurity practices. This toolkit serves as a starting point, a collection of essential resources to empower CSOs to enhance their digital security.

Cybersecurity is a journey, not a one-time task. By prioritizing cybersecurity and continuously updating your knowledge and practices, your organization can better protect itself against the ever-evolving landscape of cyber threats. Let this toolkit be the first step towards a more secure and resilient digital presence for your organization.

# **Cybersecurity Terminologies and Glossaries**

Here's a list of common cybersecurity terms with simple definitions to help you understand the basics:

1. **Malware**: Bad software designed to harm or secretly access a computer or network without the user's permission.
2. **Phishing**: A trick where attackers send fake messages (usually emails) trying to get you to reveal personal information like passwords or credit card numbers.
3. **Ransomware**: A type of malware that locks your computer or files and demands payment to unlock them.
4. **Firewall**: A digital barrier that blocks unauthorized access to your computers and devices while allowing permitted communication to pass.
5. **VPN (Virtual Private Network)**: A tool that makes your internet connection more secure by hiding your online activity and location.
6. **Two-Factor Authentication (2FA)**: An extra layer of security used to ensure that people trying to gain access to an online account are who they say they are. First, a user will enter their password, and then they must provide another piece of information.
7. **Encryption**: Turning information into a code to prevent unauthorized access. It's like sending a secret message only the intended receiver can read.
8. **Cybersecurity**: Protecting computers, networks, programs, and data from unauthorized access or attacks that are aimed for exploitation.
9. **Social Engineering**: Tricks attackers use to get people to share personal information or break security procedures.
10. **Antivirus Software**: A program designed to search for, detect, and remove software viruses and other malicious software.
11. **Patch**: A piece of software designed to update a computer program or its supporting data to fix or improve it. This includes fixing security vulnerabilities and other bugs.
12. **Data Breach**: A security incident in which information is accessed without authorization. It can involve sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.
13. **SSL/TLS (Secure Sockets Layer/Transport Layer Security)**: Protocols for establishing authenticated and encrypted links between networked computers. It's most commonly seen in secure web browsing (HTTPS).
14. **DDoS Attack (Distributed Denial of Service)**: An attempt to make an online service unavailable by overwhelming traffic from multiple sources.
15. **Zero-Day Exploit**: A hole in software that is unknown to the vendor. Hackers exploit this security vulnerability before the vendor becomes aware and hurries to fix it.

Understanding these terms will help you navigate the world of cybersecurity more effectively and enable you to take the right steps to protect yourself and your organization.

# **Cybersecurity Q&A for Civil Society Organizations**

Q1: What is Cybersecurity?

**A:** Cybersecurity is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's about keeping your information and technology safe from people who want to steal or damage it.

Q2: Why is Cybersecurity Important for Civil Society Organizations?

**A:** For civil society organizations, cybersecurity is crucial because it protects sensitive data, maintains the privacy of members and beneficiaries, and ensures the continuity of their operations. A breach could result in the loss of trust, financial damage, or even put individuals at risk.

Q3: What Are Some Common Cyber Threats?

**A:** The most common threats include malware (like viruses and ransomware), phishing attacks, data breaches, and denial of service attacks. These threats can lead to the loss of sensitive information, financial damage, and disruption of services.

Q4: How Can We Create Strong Passwords?

**A:** Strong passwords are long (at least 12 characters), include a mix of letters (upper and lower case), numbers, and symbols, and should not contain easily guessed information. It’s also important to use different passwords for different accounts. More tips are available in the "Secure Password Creation and Management Tools" section of this toolkit.

Q5: What is Two-Factor Authentication (2FA), and Should We Use It?

**A:** 2FA adds an extra layer of security by requiring two types of information before you can access an account: something you know (like a password) and something you have (like a code sent to your phone). It's highly recommended to use 2FA to protect sensitive accounts.

Q6: What Should We Do If We Suspect a Cybersecurity Incident?

**A:** If you suspect an incident, immediately report it to your IT department or cybersecurity point of contact. Disconnect the affected device from the internet if possible. Do not delete or tamper with any potential evidence. Follow the steps outlined in the "Incident Response Plan Template" section of this toolkit.

Q7: How Can We Improve Our Organization’s Cybersecurity?

**A:** Educate your employees about cybersecurity threats and best practices, keep your software and systems updated, use antivirus software, secure your internet connections, and develop and follow a comprehensive incident response plan. Regular training and awareness can significantly improve your cybersecurity posture.

Q8: Are There Any Free Resources for Cybersecurity Training?

**A:** Yes, there are several free resources available online for cybersecurity training, including materials from the Cybersecurity and Infrastructure Security Agency (CISA), online courses on platforms like Coursera and edX, and various cybersecurity awareness websites. Refer to the "Essential Cybersecurity Training for Employees" section for more details.

Q9: How Can Social Media be Used Safely?

**A:** To use social media safely, adjust your privacy settings, think before you post, use strong passwords, enable 2FA, and be cautious about clicking links. More guidelines can be found in the "Social Media Security Awareness" section of this toolkit.

Q10: Where Can We Find More Information on Cybersecurity?

**A:** For a deeper understanding, consider exploring the resources mentioned throughout this toolkit, attending cybersecurity webinars and workshops, and consulting the websites of reputable cybersecurity organizations. Engaging with online communities and forums can also provide valuable insights and updates on the latest threats and protection strategies.

This Q&A aims to address the basic and slightly more advanced cybersecurity questions relevant to civil society organizations. By familiarizing yourself with these concepts and practices, your organization can significantly reduce its vulnerability to cyber threats and ensure a safer digital environment for its operations and data.

# **Cybersecurity Awareness Resources**

To support civil society organizations in Afghanistan in bolstering their cybersecurity defenses in a non-technical, accessible manner, developing a suite of practical, user-friendly resources is proposed. These resources aim to enhance cybersecurity awareness and preparedness among employees who may need to gain more expertise in computers or cybersecurity.

**1. Cybersecurity Awareness Posters**

* Simple, visually engaging posters that highlight key cybersecurity practices, such as creating strong passwords, identifying phishing emails, and securing devices. These can be placed around the office for constant visibility.

**2. Safe Internet Use Guidelines**

* A straightforward guide on safe browsing practices, identifying secure websites, and the importance of avoiding suspicious links and downloads.

**3. Email Security Checklist**

* A checklist for safely managing emails, including tips on how to recognize phishing attempts, handle unknown attachments, and use email encryption when necessary.

**4. Data Protection and Privacy Guide**

* An easy-to-understand guide on protecting personal and organizational data, including the use of VPNs, secure file-sharing practices, and the basics of data encryption.

**5. Incident Response Plan Template**

* A simple template to help organizations prepare for and respond to cybersecurity incidents, including steps to contain, eradicate, and recover from common threats like malware or data breaches.

**6. Device Security Best Practices**

* A guide outlining basic security measures for computers and mobile devices, such as installing antivirus software, enabling firewalls, and keeping software up to date.

**7. Secure Password Creation and Management Tools**

* A resource explaining how to create strong, unique passwords and the importance of using a password manager.

**8. Social Media Security Awareness**

* Tips and best practices for securing social media accounts and understanding privacy settings to protect organizational and personal information.

**9. Cybersecurity Training Webinars**

* Recorded, easy-to-follow webinars covering essential cybersecurity topics that employees can watch at their convenience to improve their understanding and awareness.

**10. Regular Cybersecurity Updates and Alerts**

* A subscription-based, regular update service (e.g., monthly emails) that informs organizations of the latest cybersecurity threats and how to avoid them.

**11. Two-Factor Authentication (2FA) Setup Guide**

* A non-technical guide explaining the importance of 2FA and step-by-step instructions on how to enable it for various services.

**12. Digital Literacy Workshops**

* Interactive workshops aimed at improving overall digital literacy, focusing on the safe and effective use of the internet and digital tools for work.

These resources will be designed with clear, concise language and visual aids to ensure they are accessible to all employees, regardless of their technical background or language proficiency. The goal is to empower individuals within these organizations with the knowledge and tools they need to protect themselves and their work from cyber threats.

# **Daily Digital Security Routine Checklist**

* **Essential Updates:** Check for and apply updates to operating systems, all software, and firmware on network devices.
* **Critical Backups:** Perform scheduled backups of essential data (cloud/local, depending on your setup). Quickly verify backup success.
* **Access Review:** Conduct a quick spot-check of user accounts. Investigate if any new accounts have been created without authorization.
* **Monitor Network:** Look for abnormalities in network traffic, especially anomalies in volume or connections from/to unfamiliar locations.
* **Password Hygiene:** Enforce a rotating password change schedule (e.g., every 90 days). If you notice compromised credentials, reset them immediately.
* **Secure Messaging:** Prioritize encrypted channels for confidential information when emailing, messaging, or video conferencing.
* **Phishing Alertness:** Train yourself to spot suspicious emails and links. Don't hesitate to report anything potentially malicious to your IT team.
* **Social Media Hygiene:** Quick check of privacy settings across platforms. Look for unusual posts or content you didn't authorize.

# **Essential Cybersecurity Training for Employees**

To ensure that all employees are equipped to protect themselves and their organization from cyber threats, it's crucial to have a structured training plan in place. This training should be part of the onboarding process and be revisited regularly, at least once a year, to keep everyone updated on new threats and best practices. Here's a guide on why such a plan is important, potential training topics, and resources for conducting these trainings.

Why a Structured Cybersecurity Training Plan Is Important

* **Raises Awareness**: Regular training raises awareness of cybersecurity threats and the role each employee plays in defending against them.
* **Updates on Threats**: Cyber threats evolve rapidly. Continuous training helps employees stay informed about new threats and how to avoid them.
* **Builds a Security Culture**: Training fosters a culture of security within the organization, making it a shared responsibility.
* **Reduces Risks**: Educated employees make smarter decisions, reducing the risk of cyber incidents.

Topics to Be Discussed

1. **Understanding Cyber Threats**: Overview of malware, phishing, social engineering, ransomware, and other common threats.
2. **Password Security and Management**: Best practices for creating and managing strong passwords.
3. **Email Security**: Identifying and avoiding phishing and scam emails.
4. **Internet and Social Media Safety**: Safe browsing practices and the risks of oversharing on social media.
5. **Mobile Device Security**: Securing personal and work-related devices.
6. **Protecting Sensitive Information**: Best practices for handling and sharing sensitive data.
7. **Incident Reporting and Response**: How to report suspected security incidents and the basic response protocol.

Free Online Resources

* **Cybersecurity and Infrastructure Security Agency (CISA)**: Offers various cybersecurity resources and training for free.
* **National Institute of Standards and Technology (NIST)**: Provides comprehensive guidelines and educational materials on cybersecurity.
* **Coursera and edX**: Host free courses on cybersecurity fundamentals from universities and colleges.

Other Options (Fee-Based)

* **Professional Cybersecurity Training Providers**: Offer in-depth courses and certifications for a fee. These can range from beginner to advanced levels.
* **Customized Workshops**: Hiring a cybersecurity expert to conduct workshops tailored to your organization's specific needs and threats.
* **Online Learning Platforms**: Platforms like LinkedIn Learning or Udemy offer courses on cybersecurity topics for a subscription fee or on a per-course basis.

Implementing the Plan

* **Mandatory Training**: Make cybersecurity training mandatory for all new hires and schedule annual refresher courses for all staff.
* **Engage and Test**: Use engaging content like videos, quizzes, and interactive workshops. Consider conducting simulated phishing exercises to test employees' knowledge.
* **Track Completion and Feedback**: Keep records of who has completed the training. Gather feedback to improve future sessions.

# **Secure Password Creation and Management Tools**

Creating and managing secure passwords is essential to protect your personal and work information from being stolen or misused. Here is a simple guide to help you create strong passwords and manage them effectively:

Creating Strong Passwords

1. **Make It Long**: Aim for at least 12 characters. Longer passwords are harder for thieves to crack.
2. **Use a Mix of Characters**: Combine letters (both uppercase and lowercase), numbers, and symbols to make your password stronger.
3. **Avoid Obvious Choices**: Don't use easily guessed information like your name, "password," dates, or repeated characters.
4. **Be Unique**: Create a different password for each account. If one password is stolen, your other accounts remain safe.

Keeping Your Passwords Safe

1. **Don’t Share Them**: Keep your passwords to yourself. Don’t share them with friends or coworkers.
2. **Change Regularly**: Change your passwords every few months, especially for important accounts like email and banking.
3. **Beware of Phishing Scams**: Never enter your password on a site you've reached by clicking a link in an email. Always go directly to the website by typing its address.

Tips and Tricks

* **Use Phrases**: Think of a sentence or a phrase you can remember easily and use the first letters of each word, mixing in numbers and symbols. For example, "I love to eat pizza on Fridays!" could become "Il2epoF!"
* **Avoid Common Substitutions**: Password crackers are wise to common substitutions (like "pa$$word"). They don't add much security, so focus on randomness and length instead.

Password Management Tools

Since remembering all your strong, unique passwords can be challenging, consider using a password manager. These tools can:

* **Generate Strong Passwords**: Automatically create secure passwords for you.
* **Store Passwords Securely**: Keep all your passwords in one encrypted and password-protected vault.
* **Auto-Fill Passwords**: Enter your passwords for you when you log in to websites and apps.

**Best Practices for Using Password Managers**

1. **Choose a Reputable Tool**: Pick a password manager with good reviews and a strong security record.
2. **Use a Strong Master Password**: This is the one password you need to remember, so make it especially strong.
3. **Enable Two-Factor Authentication (2FA)**: If your password manager offers it, turn on 2FA for an extra layer of security.

By following these guidelines, you can greatly improve your cybersecurity posture and protect your personal and professional information from unauthorized access.

# **Email Security Best Practices Checklist**

1. **Use Strong Passwords**: Combine letters, numbers, and symbols.
2. **Enable Two-Factor Authentication (2FA)**: Add an extra layer of security.
3. **Beware of Phishing Attempts**: Don’t click on unknown links or attachments.
4. **Use Secure Connections**: Prefer encrypted (SSL/TLS) connections.
5. **Regularly Update Email Software**: Keep your email client and security software up to date.
6. **Encrypt Sensitive Emails**: Use email encryption tools for confidential information.
7. **Avoid Public Wi-Fi for Accessing Email** Or use a VPN if necessary.
8. **Regularly Review Account Access and Activity**: Monitor for unauthorized access.
9. **Educate Yourself and Team**: Stay informed about the latest email threats.
10. **Backup Important Emails**: Use a secure method for backing up important communications.

*User Note*: This checklist provides foundational steps for securing email communications. Customize and expand based on your organization's specific needs, policies, and the sensitivity of the information you handle. Regular review and adherence to these practices are crucial for maintaining email security.

# **Mobile Device Security Checklist**

1. **Enable Screen Lock**: Use a PIN, password, or biometric lock.
2. **Install Security Apps**: Use reputable antivirus and anti-theft apps.
3. **Update Regularly**: Keep the operating system and apps up to date.
4. **Use Secure Wi-Fi**: Avoid public Wi-Fi or use a VPN.
5. **Enable Encryption**: Encrypt data stored on your device.
6. **Be App-Wise**: Download apps from official stores only.
7. **Disable Bluetooth**: When not in use, turn off Bluetooth.
8. **Backup Data**: Regularly backup important data.
9. **Beware of Phishing**: Don’t click on suspicious links in emails or messages.
10. **Remote Wipe Capability**: Set up the ability to remotely erase data if lost.

*User Note*: This checklist offers a starting point for securing mobile devices within your organization. Tailor these recommendations to fit specific device types and operational needs, ensuring comprehensive protection against mobile security threats.

# **Social Media Security Awareness Guide**

Social media is a powerful tool for staying connected and sharing information, but it also presents significant security risks if not used cautiously. For civil society organizations and their employees, understanding how to navigate social media safely is crucial. Here’s a simple guide on social media security awareness:

Understanding the Risks

1. **Personal Information Exposure**: Sharing too much personal information can put you and your organization at risk.
2. **Phishing Scams**: Cybercriminals use social media to trick people into giving away sensitive information.
3. **Account Hijacking**: Weak passwords and a lack of security measures can allow hackers to take over social media accounts.
4. **Malware and Viruses**: Clicking on malicious links shared on social media can infect your device with harmful software.

Best Practices for Social Media Security

1. **Privacy Settings**: Regularly check and adjust your privacy settings to control who can see your posts and personal information.
2. **Think Before You Share**: Be mindful of what you post online. Avoid sharing sensitive personal or organizational information.
3. **Strong Passwords**: Use strong, unique passwords for each of your social media accounts. Consider using a password manager to keep track of them.
4. **Enable Two-Factor Authentication (2FA)**: Adding an extra layer of security can significantly reduce the risk of unauthorized access to your accounts.
5. **Be Skeptical**: Don’t click on suspicious links, even if they appear to come from friends. When in doubt, verify through another communication channel.
6. **Regular Monitoring**: Keep an eye on your account for any unusual activity, such as posts you didn’t make or messages you didn’t send.
7. **Educate and Inform**: Share your knowledge with colleagues. The more informed everyone is, the safer your organization will be.

Handling Suspicious Activity

* **Act Immediately**: If you suspect your account has been compromised, change your password immediately and notify the social media platform.
* **Inform Your Organization**: If the compromised account is related to your work, inform your organization’s IT or security team.
* **Review Account Activities**: Check for any posts, messages, or changes made during the period your account was compromised and revert any unauthorized changes.

Resources for Further Learning

* Consider participating in online courses or webinars focused on digital literacy and cybersecurity.
* Follow reputable cybersecurity organizations on social media for updates and tips.

By following these guidelines, individuals and organizations can enjoy the benefits of social media while minimizing the risks. Encouraging a culture of security awareness and vigilance can protect against potential threats and ensure a safer online environment for all.

# **Cybersecurity for Remote Workers: A Guide**

In today’s digital world, remote work has become increasingly common. However, working outside the traditional office environment presents unique cybersecurity challenges. This guide provides essential tips and best practices to help remote workers and their organizations stay secure online.

Establish Secure Connections

* **Use a Virtual Private Network (VPN):** A VPN creates a secure connection over the internet to your organization’s network. Always use a VPN when accessing work resources from home or public Wi-Fi.
* **Secure Your Wi-Fi Network:** Ensure your home Wi-Fi is secured with a strong password. Avoid using public Wi-Fi for work-related tasks whenever possible.

Manage Passwords Effectively

* **Use Strong, Unique Passwords:** Each account should have a unique password that is complex and difficult to guess.
* **Leverage a Password Manager:** A password manager can help you manage different passwords securely and make it easier to use strong, unique passwords for each service.

Keep Software and Systems Updated

* **Regular Updates:** Keep your operating system, applications, and any work-related software updated to protect against the latest threats.
* **Use Antivirus Software:** Ensure that you have reputable antivirus software installed and that it is set to update automatically.

Be Vigilant Against Scams

* **Recognize Phishing Attempts:** Be cautious of emails or messages requesting sensitive information or urging you to click on links or download attachments. When in doubt, verify the request through another communication method.
* **Report Suspicious Activities:** If you encounter anything suspicious, report it to your organization’s IT or security team immediately.

Secure Your Work Environment

* **Physical Security:** Ensure that your devices are in a secure location where they cannot be accessed or stolen by others.
* **Data Privacy:** Be mindful of your surroundings, especially if you work in public spaces. Use privacy screens and headphones to protect information from being seen or heard by others.

Use Secure Communication Tools

* **Approved Tools Only:** Use communication tools and platforms approved by your organization. Avoid discussing sensitive work matters on unsecured or personal platforms.

Backup Data Regularly

* **Regular Backups:** Ensure that your work data is backed up regularly. Follow your organization’s policy for backing up data, whether it’s to a cloud service or an external hard drive.

Remote Work Policy Compliance

* **Understand Your Organization’s Policy:** Be familiar with and adhere to your organization’s remote work and cybersecurity policies.
* **Security Training:** Participate in any cybersecurity training offered by your organization to stay updated on best practices and policies.

**User Notes**

* **Customization:** Adapt these practices to fit your specific work situation and the level of risk associated with your job.
* **Communication:** Keep in constant communication with your team and IT department about any cybersecurity concerns or incidents.
* **Education:** Stay informed about the latest cybersecurity threats and trends. Regularly seek out information and training to improve your security posture.

By following these guidelines, remote workers can significantly reduce their cybersecurity risks and contribute to the overall security of their organization. Remember, cybersecurity is a shared responsibility, and staying informed and vigilant is key to protecting yourself and your organization from cyber threats.

# **Digital Hygiene Best Practices**

Digital hygiene refers to the practices and habits that users follow to maintain the health and security of their digital presence. Just like personal hygiene keeps you healthy, digital hygiene helps keep your online activities safe and secure. Here are some best practices to enhance your digital hygiene:

Keep Software Up to Date

* **Regular Updates:** Ensure that all your devices (computers, smartphones, tablets) have the latest software updates, including operating systems and applications. These updates often include security patches.

Use Strong Passwords and Manage Them Wisely

* **Strong Passwords:** Use passwords that are long, complex, and unique for each account. Incorporate letters, numbers, and symbols.
* **Password Managers:** Consider using a password manager to store and manage your passwords securely.

Be Cautious with Emails and Links

* **Phishing Awareness:** Be vigilant about phishing attempts. Do not click on links or download attachments from unknown or suspicious emails.
* **Verify Sources:** If unsure about an email's legitimacy, contact the sender directly through a different communication channel.

Secure Your Internet Connection

* **Use a VPN:** A Virtual Private Network (VPN) encrypts your internet connection, protecting your data from eavesdroppers, especially on public Wi-Fi networks.
* **Wi-Fi Security:** At home, secure your Wi-Fi network with a strong password and WPA2 or WPA3 encryption.

Protect Sensitive Information

* **Limit Sharing:** Be mindful of the personal information you share online, especially on social media. Adjust privacy settings to control who can see your information.
* **Data Encryption:** Use encryption for sensitive files and communications. Many messaging apps now offer end-to-end encryption.

Regularly Backup Your Data

* **Backup Strategy:** Regularly back up important data to an external drive or cloud storage. This protects your information in case of data loss or a ransomware attack.

Be Aware of Your Digital Footprint

* **Online Behavior:** Remember that most of what you do online leaves a trace. Be conscious of the information you post and the websites you visit.
* **Review Permissions:** Regularly review the permissions you've granted to apps and websites, especially those accessing your location, camera, or contact list.

Use Security Software

* **Antivirus Protection:** Install reputable antivirus software to protect against malware. Set it to update automatically.
* **Firewalls:** Use a firewall on your computer to block unauthorized access to your network and devices.

Educate Yourself and Others

* **Stay Informed:** Keep up with the latest cybersecurity threats and trends. Knowledge is a powerful tool in preventing cyber attacks.
* **Share Knowledge:** Educate friends, family, and colleagues about the importance of digital hygiene and how they can protect themselves.

**User Notes**

* **Customization:** Adapt these practices to fit your personal and organizational needs. Not every recommendation may be necessary or practical for every individual or situation.
* **Consistency:** Digital hygiene is not a one-time task but a continuous process. Regularly review and update your practices.
* **Proactivity:** Being proactive about your digital hygiene can prevent many common cyber threats and protect your personal and professional data.

By adopting these digital hygiene best practices, individuals and organizations can significantly improve their online security posture and resilience against cyber threats.

# **Cybersecurity Policy Template for Organizations**

A simple template to help organizations draft their own cybersecurity policy. This document would outline the organization's stance on cybersecurity, including acceptable use of technology, security protocols, data protection measures, and responsibilities of staff and management.

**Quick Cybersecurity Checkup Checklist**

A straightforward checklist that organizations can use regularly (e.g., monthly or quarterly) to ensure they are following basic cybersecurity practices. It would cover areas such as password policies, software updates, backup verification, and incident reporting mechanisms.

**Guide to Conducting Cybersecurity Awareness Sessions**

A step-by-step guide for organizations to conduct their own internal cybersecurity awareness sessions. This guide would include tips on organizing the session, key topics to cover, engaging activities to include, and how to measure the effectiveness of the session.

**Cybersecurity for Remote Workers**

With the rise of remote work, a dedicated guide on cybersecurity practices for remote workers would be highly beneficial. This guide will cover secure home networks, the importance of VPNs, secure use of personal devices for work, and tips for preventing unauthorized access to data.

**Digital Hygiene Best Practices**

A resource focusing on daily habits and practices that enhance cybersecurity. This would include guidance on managing digital footprints, safely using public Wi-Fi, secure browsing practices, and understanding app permissions on mobile devices.

These additional resources would further strengthen the toolkit, providing civil society organizations with a comprehensive set of materials to enhance their cybersecurity posture and awareness in a non-technical, accessible manner.

# **Cybersecurity Template for Organizations**

**Organization Name:** [Your Organization Name Here]

**Document Version:** 1.0

**Date:** [Date Here]

**Prepared by:** [Your Name/Position Here]

**I. Introduction**

This cybersecurity policy outlines the measures [Your Organization Name Here] takes to protect its information technology systems and data from cybersecurity threats. It applies to all employees, contractors, and volunteers.

**II. Purpose**

The purpose of this policy is to ensure the integrity, confidentiality, and availability of [Your Organization Name Here]'s data and technology infrastructure.

**III. Scope**

This policy applies to all users of [Your Organization Name Here]'s information systems and networks, including but not limited to employees, contractors, and volunteers.

**IV. Policy Statements**

1. **User Access Control**
	* Users must have individual accounts and passwords.
	* Access to sensitive data is restricted to authorized personnel only.
2. **Password Management**
	* Passwords must be strong, at least 12 characters long, and include a mix of letters, numbers, and symbols.
	* Passwords must be changed every [specify period, e.g., 90 days].
3. **Data Protection**
	* All sensitive data must be encrypted.
	* Data backups must be performed regularly.
4. **Incident Response**
	* Any suspected security incidents must be reported immediately to [specify role/title].
	* A documented incident response plan must be followed in the event of a security breach.
5. **Software and Systems**
	* All software must be licensed and kept up-to-date with the latest security patches.
	* The use of unauthorized software is prohibited.
6. **Network Security**
	* Firewalls and antivirus software must be used to protect against external threats.
	* The use of public Wi-Fi for work-related tasks must be done through a VPN.
7. **Email and Communication Security**
	* Phishing awareness training will be provided to all users.
	* The use of email for transmitting sensitive information is discouraged unless encrypted.
8. **Mobile Device and Remote Work Security**
	* Devices accessing organizational data must have security measures, such as encryption and password protection.
	* Remote work must be conducted in accordance with the organization's remote work policy.

**V. Enforcement**

Violations of this policy may result in disciplinary action, up to and including termination of employment or contracts.

**VI. Review and Revision**

This policy will be reviewed annually and updated as necessary to reflect changes in technology, threats, and organizational priorities.

**User Notes**

* **Adopting the Policy:** Customize this template with your organization's specific details, practices, and requirements. Consider your organization's unique cybersecurity challenges and needs when filling in the sections.
* **Implementing the Policy:** Effective implementation requires communicating the policy to all relevant parties, providing necessary training, and establishing processes for monitoring compliance.
* **Updating the Policy:** Cybersecurity is a rapidly evolving field. Regularly review and update the policy to incorporate new technologies, threats, and best practices. Feedback from users can be invaluable in identifying areas for improvement.

This template provides a foundation for developing a cybersecurity policy tailored to the needs of civil society organizations. It's important to ensure that the policy is accessible and understood by all members of the organization, regardless of their technical expertise.

# **Digital Security Policy Template for CSOs**

**I. Purpose and Scope**

* **Purpose:** Clearly articulate the reasons for the policy (protect assets, comply with regulations, safeguard reputation, etc.).
* **Scope:** Define what the policy encompasses (data, systems, users, networks, vendors) and any specific exclusions.
* **Applicability:** State who must adhere to the policy (employees, contractors, third parties).

**II. Policy Principles**

* **Confidentiality:** Protection of sensitive data from unauthorized access.
* **Integrity:** Maintaining data accuracy and completeness and preventing unauthorized modification.
* **Availability:** Ensuring systems and data are accessible to authorized users when needed.
* **Compliance:** Adherence to legal, regulatory, and contractual obligations.
* **Risk-Based Approach:** Implementing security measures aligned with identified risks.
* **Continuous Improvement:** Regularly review and update the policy based on evolving threats and business needs.

**III. Roles and Responsibilities**

* **CSO:** Ultimate responsibility for developing, implementing, and enforcing the policy.
* **IT Security Team:** Day-to-day maintenance and monitoring of security systems.
* **Department Heads:** Responsibility for security implementation within their areas.
* **Employees:** Compliance with policies and reporting potential security concerns.
* **Vendors/Partners:** Adherence to the organization's security standards when sharing data.

**IV. Data Protection**

* **Data Classification:** Define sensitivity levels (e.g., confidential, internal, public) and handling rules for each.
* **Encryption:** Enforce encryption at rest and in transit for sensitive data. Specify allowed encryption protocols and strengths.
* **Storage:** Approved storage locations and methods (e.g., cloud restrictions, prohibited devices).
* **Retention:** Data retention periods in alignment with legal and business needs.
* **Disposal:** Secure disposal procedures for physical and digital data.

**V. Access Control**

* **Authentication:** Strong password policies (length, complexity, reuse, expiration), mandatory MFA where feasible.
* **Authorization:** Principle of least privilege and regular user access reviews.
* **Account Management:** Processes for creating, deactivating, and modifying user accounts.
* **Privileged Access:** Tighter controls, monitoring, and auditing for administrative accounts.

**VI. Network Security**

* **Firewalls:** Hardware and software firewall requirements configuration rules.
* **VPNs:** Mandatory use for remote access and approved VPN solutions.
* **Wi-Fi:** Strong encryption, limiting signal range, segregated guest networks.
* **Antivirus/Anti-Malware:** Approved software, update schedules, scan settings.
* **Patch Management:** Timely patching of OS, applications, and network devices.
* **Intrusion Detection/Prevention:** Use of IDS/IPS where appropriate.

**VII. Incident Response**

* **Definition of Incident:** Examples of incidents (data breach, malware, unauthorized access).
* **Reporting:** Reporting chain of command, timelines, and contact information.
* **Containment:** Procedures for isolating affected systems and data.
* **Investigation and Analysis:** Root cause analysis and evidence collection.
* **Eradication:** Steps for removing threats and patching vulnerabilities.
* **Recovery:** Data restoration, testing, and returning systems to operation.
* **Communication:** Internal and external stakeholders, legal/regulatory reporting.
* **Post-Incident Review:** Lessons learned, policy and process improvement.

**VIII. Training and Awareness**

* **Mandatory Training:** Initial and recurring security training for all employees.
* **Content:** Passwords, phishing, safe browsing, incident reporting, social engineering.
* **Training Methods:** Variety of delivery methods (in-person, online, simulations).
* **Documentation:** Records of training attendance and completion.

**IX. Review and Updates**

* **Review Schedule:** At least annual review or after significant changes (threats, business).
* **Responsibility:** Designated responsible party for conducting the review.
* **Update Process:** Procedure for policy change approvals and communication.

**Additional Considerations for Your Policy**

* **Physical Security:** Access restrictions to hardware, badges, cameras, and visitor logs.
* **Removable Media:** Policies for USB drives, external disks, and data transfers.
* **Mobile Device Security:** Allowed devices, secure configurations, and remote wiping capability.
* **Cloud Security:** Approved cloud providers' security requirements for SaaS.
* **Vendor Risk Management:** Assessment process for vendor security practices.
* **Incident Severity Levels:** Clearly define criteria for categorizing incidents (might influence response plans).

**Employee Agreement on Digital Security Practices**

* **Acknowledgment:** Signature verifying the employee read and understands the policy.
* **Compliance:** Agreement to abide by all specified procedures and guidelines.
* **Reporting:** Commitment to promptly report any suspected breaches or unusual activity.
* **Confidentiality:** Understanding of non-disclosure obligations related to company data.
* **Personal Devices:** If allowed for work, restrictions on what is permissible.
* **Consequences:** Clearly outline disciplinary actions up to and including termination for violations.

**Digital Incident Report Form**

* **Incident Details:** Date, time, location, systems/data affected, brief description, type (phishing, malware, unauthorized access, etc.).
* **Impact:** Business disruption, estimated damages, potential regulatory fines.
* **Discovery:** How and by whom was the incident detected?
* **Initial Containment:** Steps taken to isolate affected systems/block the spread.
* **Reporter Info:** Full name, title, contact info, department.
* **Escalation:** Who was notified, any immediate corrective actions beyond containment.
* **Detailed Incident Narrative:** Area for thorough documentation of the events as they unfolded.
* **Evidence Preservation:** Log files, screenshots, etc. (attach separately as needed).
* **Lessons Learned:** Space for analysis after the incident is fully resolved.

**Improvements**

* **Make it Actionable:** Use clear verb-driven language (e.g., "Employees must..." instead of "Employees should...").
* **Avoid Excessive Jargon:** Define technical terms or provide a glossary to promote wider understanding.
* **Tailor it:** Customize the policy to your organization's specific risks and requirements.

**Key Notes**

* Communicate the policy effectively to all relevant individuals.
* Obtain signatures on the 'Employee Agreement' form.

Regularly test your Incident Response Plan to make sure it functions in practice

# **Digital Security Policy Template (Short Version)**

**[Organization Name] Digital Security Policy**

**Effective Date:** [Date]

**1. Introduction** This Digital Security Policy outlines [Organization Name]'s commitment to protecting digital assets and sensitive information against cyber threats. It applies to all employees, volunteers, and partners.

**2. Purpose** To ensure the confidentiality, integrity, and availability of digital assets and to comply with legal and ethical standards.

**3. Scope** Covers all digital systems, data, and communication used by the organization.

**4. Policy Principles**

* **Data Protection:** Implement encryption for sensitive data storage and transmission.
* **Access Control:** Access to data and systems is based on roles and necessity.
* **Incident Response:** Establish a protocol for responding to and managing security incidents.

**5. Roles and Responsibilities**

* **Management:** Approve and enforce the digital security policy.
* **Employees/Volunteers:** Adhere to digital security practices.
* **IT Department:** Implement and monitor security measures.

**6. Policy Enforcement** Violations of this policy may result in disciplinary action, up to and including termination of employment or partnership.

**7. Review and Updates** This policy will be reviewed annually or as needed to reflect changes in technology or threats.

**[Organization Name]**

*[Date]*

**Employee Agreement on Digital Security Practices**

**[Employee/Volunteer Name] Agreement on Digital Security Practices**

**I, [Name], acknowledge the importance of adhering to [Organization Name]'s Digital Security Policy to protect against digital threats.**

**1. Compliance:** I will comply with all aspects of the Digital Security Policy, including but not limited to, secure password practices, data encryption, and incident reporting.

**2. Reporting:** I commit to immediately reporting any security incidents or vulnerabilities I become aware of.

**3. Confidentiality:** I will maintain the confidentiality of sensitive information at all times.

**4. Consequences:** I understand that failure to comply with these practices may result in disciplinary action.

**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# **Data Protection Policy Template**

**[Organization Name]**

**Effective Date:** [Date]

**1. Purpose:** Outlines the organization's commitment to protecting personal and sensitive data in compliance with applicable laws and best practices.

**2. Scope:** Applies to all employees, volunteers, and third parties who handle data on behalf of the organization.

**3. Principles of Data Protection:** Adheres to principles such as lawfulness, fairness, transparency, accuracy, data minimization, and accountability in data processing.

**4. Rights of Data Subjects:** Describes the rights of individuals regarding their data, including access, correction, deletion, and objection to processing.

**5. Data Security Measures:** Details technical and organizational measures to protect data against unauthorized access, disclosure, alteration, and destruction.

**6. Breach Notification:** Establishes procedures for responding to data breaches, including timely notification to authorities and affected individuals.

**7. Roles and Responsibilities:** Defines roles within the organization for overseeing data protection, including the appointment of a Data Protection Officer (DPO) if necessary.

**8. Training and Awareness:** Commits to providing regular data protection training to all relevant personnel.

**9. Policy Review and Update:** Specifies intervals for reviewing and updating the policy.

**Approval:**

[Authorized Signature] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_

# **Incident Response Plan Template**

When bad things happen to our computer systems or data, it's important to have a plan so we know what to do. This plan is called an "Incident Response Plan." It helps us act quickly and correctly to stop the harm and fix what went wrong. Here's a simple plan you can use:

Part 1: What to Do First

1. **Know Who to Tell**: Have a list of people or teams who need to know as soon as something bad happens. This might include your boss, IT support, and anyone else important.
2. **Stay Calm and Gather Info**: Write down what happened, what you saw, and any changes you noticed in your computer or emails. This info can help fix things.

Part 2: Stopping the Problem

1. **Disconnect from the Internet**: If your computer is acting strangely, disconnect it from the Internet. This can stop the problem from spreading.
2. **Don’t Delete Anything Yet**: It might feel right to delete weird emails or files, but don’t. Save everything as it is. It can help figure out what happened later.

Part 3: Fixing the Damage

1. **Call in Experts**: If you have IT support, let them take over. They know how to clean and fix your computer safely.
2. **Change Your Passwords**: After talking to IT support, change your passwords, especially if you think someone else might know them.

Part 4: Learning from the Incident

1. **Talk About What Happened**: Have a meeting with your team. Discuss what happened, how it was fixed, and how you can stop it from happening again.
2. **Update Your Plan**: Use what you learned to make this plan better. Maybe you need clearer steps or more people to help.

Part 5: Important Contacts

* **IT Support Contact**: [Insert contact info]
* **Boss/Manager Contact**: [Insert contact info]
* **Security Team Contact** (if you have one): [Insert contact info]

Part 6: Practice Makes Perfect

* **Practice**: Once in a while, practice what you would do if something bad happened. This helps everyone feel more ready.

This plan is just a start. You might need to add more details based on what your organization does or the specific risks you face. The most important thing is to have a plan and make sure everyone knows what to do.

# **Security Risk Assessment Form**

**Organization Name:**

* [Organization's Name]

**Date:**

* [Assessment Date]

**Assessment Conducted By:**

* [Name and Position]

**I. Overview of Assets**

* List all digital assets (e.g., databases, applications, information systems).

**II. Identified Threats**

* Detail potential threats to each listed asset (e.g., malware, unauthorized access).

**III. Vulnerability Assessment**

* Evaluate the susceptibility of each asset to the identified threats.

**IV. Impact Analysis**

* Assess the potential impact (e.g., financial, reputational) of threats being realized.

**V. Risk Level**

* Assign a risk level (e.g., low, medium, high) to each combination of asset and threat.

**VI. Existing Controls**

* Describe current measures in place to mitigate identified risks.

**VII. Recommended Enhancements**

* List recommendations for reducing risk levels where necessary.

**VIII. Action Plan**

* Outline steps to implement recommended enhancements, including responsible parties and timelines.

**IX. Review and Approval**

* Signatures of assessment team and organizational leadership.

**Digital Tools Usage Agreement for Staff and Volunteers**

**Organization Name:**

* [Organization's Name]

**Name of User:**

* [Staff/Volunteer Name]

**Position/Role:**

* [User's Role]

**I. Acknowledgment of Policy**

* Acknowledge understanding of the organization's digital security policies.

**II. Permitted Uses**

* Detail permissible uses of organizational digital tools and resources.

**III. Prohibited Activities**

* Outline actions that are prohibited (e.g., sharing passwords, installing unauthorized software).

**IV. Security Measures**

* Agree to adhere to specified security measures (e.g., using strong passwords, encrypting sensitive data).

**V. Reporting Requirements**

* Commit to promptly reporting any security incidents or vulnerabilities discovered.

**VI. Consequences of Violation**

* Acknowledge the consequences of failing to comply with the agreement.

**VII. Agreement Duration**

* Specify the duration of the agreement's validity.

**VIII. User Acknowledgment**

* User signature and date.

**IX. Organization Approval**

* Signature of an authorized organizational representative and date.

These forms are designed to facilitate a systematic approach to assessing and mitigating digital security risks within CSOs and to ensure that staff and volunteers clearly understand and commit to upholding the organization's digital security standards.

# **Security Risk Assessment Form**

**Organization Name:**
[Insert Organization Name]

**Date:**
[Insert Date]

**Assessment Conducted by:**
[Name and Position]

**1. Asset Identification**

* **Asset Name:**
* **Description:**
* **Owner:**

**2. Threat Identification**

* **Threat Type:**
* **Potential Impact:**

**3. Vulnerability Assessment**

* **Vulnerability Description:**
* **Existing Controls:**

**4. Risk Evaluation**

* **Likelihood (High/Medium/Low):**
* **Impact (High/Medium/Low):**
* **Risk Level (High/Medium/Low):**

**5. Control Recommendations**

* **Recommended Action:**
* **Responsible Person:**
* **Deadline:**

**6. Approval**

* **Assessor's Signature:**
* **Date:**
* **Management Approval Signature:**
* **Date:**

*User Note: Adjust this form to match your organization's specific assets, threats, and control measures. Be thorough in your asset and threat identification to ensure comprehensive risk assessment.*

# **Network Security Checklist for Small Offices**

**1. Robust Wi-Fi Security**

* **Unique, Non-Identifiable SSID:** Choose a name that doesn't reveal your business or location.
* **Strong Encryption:** Always use WPA3. If unavailable, WPA2 is the *minimum* acceptable standard.
* **Complex, Regularly Changed Password:** Avoid dictionary words and change your password at least quarterly.
* **Disable WPS:** This feature is inherently vulnerable.
* **Signal Range Management:** Use router settings to limit signal reach to your office boundaries.

**2. Firewall Fundamentals**

* **Hardware Firewall:** Invest in a dedicated firewall appliance for superior perimeter protection.
* **Software Firewalls:** Enable these on all devices for individual defense.
* **Consistent Updates:** Patch firewalls religiously to combat the latest threats.

**3. Secure Remote Work with VPNs**

* **Mandate VPN Use:** Require remote employees to connect *only* through a company-provided VPN.
* **Strong VPN Encryption:** Choose a VPN service with robust encryption protocols.
* **User Education:** Train employees on proper VPN usage and the dangers of connecting to public Wi-Fi.

**4. Prioritize Updates & Patches**

* **OS, Software, & Apps:** Apply security patches promptly across all devices. Enable automatic updates whenever possible.
* **Network Equipment:** Don't neglect routers, switches, and access points—firmware updates are vital.

**5. Control Physical Access**

* **Restricted Hardware Areas:** Secure network hardware, servers, and wiring in a locked room or cabinet.
* **Device Security:** Lock workstations when unattended; use cable locks for laptops.
* **Monitoring:** Consider surveillance cameras for especially sensitive network areas.

**6. Enforce Strong Access Controls**

* **Unique, Complex Passwords:** Enforce minimum complexity standards (length, numbers, symbols) and frequent changes.
* **Multi-Factor Authentication (MFA):** Where possible, add MFA for an extra layer of security.
* **Principle of Least Privilege:** Grant users only the minimum access level they need to do their jobs.

**7. Comprehensive Endpoint Protection**

* **Reputable Anti-Virus/Anti-Malware:** Install on every device—servers, desktops, laptops.
* **Automated Updates & Scans:** Configure software for automatic updates and scheduled scans.
* **User Awareness:** Teach employees to spot phishing emails, suspicious links, and malicious attachments.

**8. Email Security Best Practices**

* **Anti-Spam & Phishing Filtering:** Leverage specialized email security services or solutions.
* **Employee Training:** Make identifying phishing a core security skill. Emphasize never opening suspicious links or attachments.
* **Encryption for Sensitive Data:** Protect confidential information in transit.

**9. Data Protection: Backups & Disaster Recovery**

* **Regular, Tested Backups:** Use a mix of cloud and local storage. Test restoration often.
* **Documented Disaster Recovery Plan:** Outline steps for data recovery, rebuilding systems, and maintaining operations during an outage.

**10. Employee Education is Paramount** - **Recurring Security Training:** Cover passwords, phishing, social engineering, safe browsing, etc. - **Clear, Enforced Policies:** Document acceptable use, incident reporting, and consequences for violations. - **Culture of Security:** Emphasize that everyone in the office is responsible for protecting the network.

**11. Proactive Incident Response** - **A Detailed Plan:** Have procedures for breach identification, containment, reporting, and remediation. - **Key Personnel & Contacts:** List internal roles and outside experts (IT, legal, etc.). - **Regular Review:** Adapt your plan as your systems and threats evolve.

**Additional Tips**

* **Network Segmentation:** Consider isolating guest Wi-Fi and untrusted devices from your core network.
* **Intrusion Detection/Prevention Systems (IDS/IPS):** Add these for advanced threat detection.
* **Regular Vulnerability Scans:** Proactively identify weaknesses and address them.

**Remember:** Cybersecurity is an ongoing process, not a one-time task. Stay vigilant and adaptable, and always make security a top priority!

# **Digital Security Audit Checklist for CSOs**

**Recurring Tasks (Weekly or Bi-Weekly)**

* **Threat Landscape Review:** Stay updated on newly discovered vulnerabilities/exploits relevant to your industry and tech stack.
* **Policy Review:** Ensure that current security policies accurately reflect business operations and risk tolerance. Update when needed.
* **Physical Access Check:** Perform a walkthrough to verify perimeter security, locking mechanisms, and access controls for server rooms/network areas.
* **Vendor Risk Assessment:** Review security certifications of critical vendors and partners. Check if they align with your security standards.

**Monthly Tasks**

* **Comprehensive Vulnerability Scan:** Schedule network-wide scans to discover potential weaknesses your daily checks might miss.
* **Employee Training Assessment:** Gauge employee retention of security procedures. Spot weaknesses and adjust training content accordingly.
* **Incident Response Drill:** Run simulations (tabletop exercises or limited live tests) to assess team preparedness and refine procedures.

**Quarterly Tasks**

* **Full Risk Assessment:** Re-evaluate your organization's digital assets, threat vectors, and priorities. Adjust security measures accordingly.
* **Deep Review of Access Controls:** Perform a thorough audit of user accounts, groups, and permissions. Enforce the principle of least privilege.
* **Data Protection Audit:** Check encryption implementation (at rest and in transit), data classification procedures, and compliance with regulations.

**Incident Response Checklist**

* **Detection & Reporting:** Have clear escalation paths. Make sure employees know when and how to report potential incidents quickly.
* **Assessment:** Define what constitutes a low, medium, and high-severity incident. Initial triage should guide the scale of your response.
* **Containment:** Predefined 'playbooks' to isolate affected systems quickly, stopping the spread.
* **Eradication:** Methodical removal of the threat, cleaning infected systems.
* **Recovery:** Restoring data from backups, bringing systems back online, and testing thoroughly.
* **Communication:** Internal and external communications plan tailored to the incident type (breach disclosure, etc.).
* **Post-Incident Review:** Root cause analysis, improvements to systems, training, or processes.
* **Documentation:** Detailed logging of the incident, the response, and the resolution.

**Important Notes:**

* The ideal frequency of some tasks depends on your organization's size and risk profile. Adjust accordingly.
* Automate recurring tasks wherever possible to increase efficiency and eliminate human error.

# **Business Continuity Planning Template tailored for CSOs, focusing on digital security measures**

1. **Introduction**: Define the purpose of the Business Continuity Plan (BCP) and its scope within your CSO.
2. **Objectives**: List the main objectives of the BCP, including ensuring service continuation during cyber threats or attacks.
3. **Risk Assessment**: Identify potential risks to digital operations and assess their impact.
4. **Critical Functions**: Determine critical services and functions that must be maintained during an incident.
5. **Response Strategies**: Outline strategies for responding to different types of cyber incidents.
6. **Recovery Plans**: Develop specific plans for the recovery of services post-incident, including data restoration and system repairs.
7. **Roles and Responsibilities**: Assign roles and responsibilities for BCP implementation and management.
8. **Communication Plan**: Establish protocols for internal and external communication during a disruption.
9. **Training and Testing**: Describe plans for training staff on BCP procedures and regularly testing the plan's effectiveness.
10. **Review and Maintenance**: Schedule periodic reviews of the BCP to ensure it remains up-to-date with evolving cyber threats.

This template serves as a foundational guide. Customize it according to your CSO's specific needs, resources, and the digital security landscape in your area.

# **Template for Partner Collaboration Agreement Including Digital Security Expectations**

**I. Introduction**

* **Purpose:** Outline the objectives of the collaboration and expected benefits.
* **Mutual Interest:** Emphasize that both partners acknowledge the critical importance of cybersecurity for the success of the collaboration.

**II. Scope of Collaboration**

* **Project Overview:** Clearly describe the type of work to be performed jointly.
* **Shared Resources:** Identify the specific IT systems, data, or networks each partner might need to access.
* **Excluded Technology:** Indicate if any highly sensitive systems or information remain off-limits to avoid misunderstandings.

**III. Digital Security Expectations**

* **Governing Standards:** Specify the security frameworks each partner agrees to follow (e.g., NIST Cybersecurity Framework, ISO 27001, SOC 2 compliance, etc.).
* **Data Encryption:** Mandate minimum encryption standards (e.g., AES-256) both at rest and during transmission of sensitive data.
* **Access Controls:** Outline how user access will be managed with a focus on the principle of least privilege. Highlight if Multi-Factor Authentication (MFA) is required.
* **Patching & Updates:** Establish a reasonable expectation for how long software can remain unpatched. Critical applications might have tighter timeframes.
* **Network Protection:** Minimum firewall requirements, the necessity of VPNs for interconnections, etc.

**IV. Data Sharing and Confidentiality**

* **Mutual NDAs:** Consider if additional non-disclosure agreements are necessary beyond this overarching agreement.
* **Data Ownership:** Clearly define which partner remains the owner of what data, even while shared during the project.
* **Data Classification:** Implement a classification system (Confidential, Restricted, Public) with corresponding handling requirements.
* **Retention and Disposal:** Agree on how long each partner can store shared data and mandate secure disposal methods upon the project's conclusion.

**V. Incident Response Coordination**

* **Primary Contacts:** Designated individuals at each organization responsible for immediate notification and cooperation in the event of an incident.
* **Escalation Procedures:** Define under what conditions executives within each organization need to become involved.
* **Communication Plan:** How updates will be exchanged during incident response and whether a common communication tool is preferred (secure messaging app, etc.).
* **Joint Review:** Commitment to post-incident review to identify improvement areas.

**VI. Compliance and Legal Obligations**

* **Applicable Regulations:** List specific laws both partners commit to complying with (GDPR, CCPA, industry-specific regulations).
* **Liability Sharing:** Clearly delineate liability in the case of a data breach. Each partner should consider having cyber-insurance aligned with this agreement.

**VII. Term and Termination**

* **Agreement Duration:** Start and end dates, automatic renewal clauses, or conditions for renewal.
* **Termination Provisions:** Under what circumstances can either partner terminate prematurely (e.g., material breach of this agreement)?
* **Data Disposition on Termination:** Procedures for return or secure deletion of any shared data upon termination.

**VIII. Review and Amendments**

* **Review Frequency:** A set schedule for formal review (annually, bi-annually).
* **Amendment Process:** How necessary changes to this security section of the agreement can be proposed and approved.

**Data Protection Policy Template (Improvements)**

* **Add Accountability:** Explicitly name who’s ultimately accountable for policy enforcement (this could be the CSO or an equivalent executive).
* **Consider Incident Response:** A brief section acknowledging that you have an Incident Response Plan aligned with this policy.

**Risk Assessment:** Mention you regularly conduct them, as these drive many of your data protection practices.

# **Digital Tools Usage Agreement for Staff and Volunteers**

**Organization Name:**
[Insert Organization Name]

**User Name:**
[Insert Name]

**Role/Position:**
[Insert Role/Position]

**Agreement Date:**
[Insert Date]

**1. Acknowledgment of Digital Security Policy**
I acknowledge that I have read and understand the organization's Digital Security Policy.

**2. Acceptable Use**
I agree to use digital tools and resources solely for professional purposes and in compliance with the policy.

**3. Prohibited Activities**
I understand that certain activities, including unauthorized access, disclosure of sensitive information, and misuse of resources, are prohibited.

**4. Security Practices**
I commit to following best practices for digital security, including password management and data protection.

**5. Incident Reporting**
I agree to immediately report any security incidents or vulnerabilities to the designated authority.

**6. Consequences of Violation**
I understand that violations of this agreement may result in disciplinary action.

**User Signature:**
[Signature]

**Date:**
[Date]

**Organization Representative Signature:**
[Signature]

**Date:**
[Date]

*User Note: This agreement should be customized to reflect your organization's specific tools, policies, and security concerns. Encourage users to ask questions if they have concerns or do not understand parts of the policy.*

# **Vulnerability Scanning and Reporting Checklist**

1. **Define Scope**: Identify systems, networks, and applications to be scanned.
2. **Select Tools**: Choose appropriate vulnerability scanning tools.
3. **Configure Scans**: Tailor scan settings to your environment.
4. **Perform Scans**: Run scans during off-peak hours to minimize impact.
5. **Analyze Results**: Review scan reports for vulnerabilities.
6. **Prioritize Remediation**: Classify vulnerabilities by severity.
7. **Fix Vulnerabilities**: Address critical vulnerabilities immediately.
8. **Document Actions**: Keep records of vulnerabilities and remediation actions.
9. **Re-scan**: Verify that vulnerabilities have been successfully mitigated.
10. **Report**: Compile and present findings to relevant stakeholders.

*User Note*: Customize the frequency and scope of scans based on your organization's size, complexity, and regulatory requirements. Regular vulnerability scanning is crucial for maintaining a strong security posture.

# **Directory of Digital Security Tools and Services**

**Purpose**: This directory is designed to help Civil Society Organizations (CSOs) in Afghanistan find and select appropriate digital security tools and services to protect their digital assets and communications.

**Usage**: Evaluate each tool or service against your specific needs, considering factors like ease of use, compatibility with your systems, and the level of security provided. Always conduct a trial or pilot phase before full implementation.

**Contents**:

1. **Encrypted Communication Tools**: List services for secure email, messaging, and voice calls.
2. **Data Encryption Software**: Options for encrypting files and databases.
3. **Antivirus and Anti-Malware Solutions**: Recommended software for protecting against malicious software.
4. **Password Managers**: Tools to generate, store, and manage secure passwords.
5. **Virtual Private Network (VPN) Services**: Providers that offer secure internet access and online privacy.

*User Note*: Regularly review and update the directory to include new tools and services that emerge in the digital security field.

**List of Contacts for Digital Security Support and Emergency Assistance**

**Purpose**: To provide CSOs with immediate access to expert advice and support in the event of a digital security breach or other cyber incidents.

**Usage**: In case of a suspected or confirmed security incident, promptly contact the listed support services for assistance in containment, eradication, and recovery. Keep this list accessible to your IT team and key staff members.

**Contents**:

1. **Digital Security Consultants**: Names, contact information, and areas of expertise.
2. **Emergency Response Teams**: Contacts for rapid response services in case of severe incidents.
3. **Legal Advisors**: Experts in digital law who can provide advice on legal obligations and responses.
4. **Training Providers**: Organizations that offer digital security training and awareness programs.

*User Note*: Ensure contacts are kept up to date and establish a relationship with service providers where possible to facilitate quicker response times in emergencies.

# **Cybersecurity Awareness Posters: A Guide**

What Are Cybersecurity Awareness Posters?

Cybersecurity awareness posters are visual tools designed to remind and educate employees about safe online behaviors and practices. They are usually colorful and straightforward, making complex cybersecurity concepts easier to understand for everyone.

The Usage of Posters

* **Educational Tool**: They provide quick tips and best practices on how to stay safe online.
* **Reminder**: Placed in common areas, they serve as constant reminders to follow cybersecurity practices.
* **Engagement**: They can spark discussions among employees about cybersecurity, enhancing overall awareness.

Benefits of Using Posters

* **Increases Awareness**: Regular exposure to these messages helps reinforce important security behaviors.
* **Accessible to Everyone**: Posters can communicate critical information at a glance, even to those not fluent in English or technical jargon.
* **Promotes a Culture of Security**: Visible commitment to cybersecurity can encourage a more security-minded workplace.

Types of Posters Needed

1. **Password Security**: Tips for creating strong passwords and the importance of not reusing them.
2. **Phishing Awareness**: How to spot phishing emails and what to do if you receive one.
3. **Internet Safety**: Guidelines for safe browsing and the risks of unsafe websites.
4. **Mobile Device Security**: Best practices for securing smartphones and tablets.
5. **Social Engineering Defense**: Tips on how to recognize and respond to social engineering attempts.
6. **Public Wi-Fi Use**: The dangers of using public Wi-Fi and how to use it safely.

What to Consider in Writing and Designing Posters

* **Simple Language**: Use easy-to-understand words and phrases.
* **Visuals**: Include engaging and relevant images or icons to illustrate points.
* **Actionable Tips**: Provide clear, actionable advice that people can follow easily.
* **Contact Information**: Include how and whom to report if they suspect a cybersecurity issue.
* **Cultural Sensitivity**: Be mindful of cultural norms and sensitivities, especially when translating.
* **Regular Updates**: Cyber threats evolve, so update your posters periodically to reflect current risks and advice.

Creating and displaying cybersecurity awareness posters can play a vital role in enhancing the overall security posture of civil society organizations, particularly in environments where technical knowledge may be limited. These posters act as both a daily reminder and an educational tool, contributing significantly to creating a safer digital work environment.

# **Data Encryption Techniques**

**Basic Principles of Data Encryption**: Data encryption transforms readable data into an unreadable format using algorithms and encryption keys. Only those with the decryption key can revert it to its original, readable form, ensuring data confidentiality and security.

**How to Encrypt Files, Databases, and Communication**:

* **Files**: Use software like VeraCrypt for disk encryption or built-in features like BitLocker (Windows) or FileVault (Mac).
* **Databases**: Implement Transparent Data Encryption (TDE), which is available in database management systems like SQL Server or Oracle.
* **Communication**: Utilize end-to-end encryption protocols in messaging apps like Signal or use SSL/TLS for securing web communications.

**5. Password Management**

**Best Practices for Creating and Managing Strong Passwords**:

* Use a mix of letters, numbers, and special characters.
* Avoid common words and phrases; opt for longer, complex passwords.
* Do not reuse passwords across different accounts.

**Use of Password Managers**: Password managers store and encrypt passwords, requiring you to remember only one master password.

* **Features**: Auto-generation of strong passwords, secure storage, auto-fill forms, and cross-platform synchronization.
* **Recommendations**: Consider reputable managers like LastPass, 1Password, or Bitwarden for their robust security features and user-friendly interfaces.

**8. Creating a Digital Security Plan**

**Steps to Develop a Comprehensive Plan**:

1. **Identify Assets**: List all digital assets (data, hardware, software).
2. **Assess Risks**: Identify potential threats and vulnerabilities to these assets.
3. **Define Security Measures**: Outline protective steps for each asset based on risk assessment.
4. **Implement Controls**: Start with high-priority areas, ensuring essential protections are in place.
5. **Training and Awareness**: Develop a plan to educate staff on their roles in digital security.
6. **Monitor and Review**: Establish ongoing monitoring of security measures and periodic reviews.

*User Note*: Adapt and expand each step based on specific organizational needs, technologies used, and evolving threat landscapes.

**9. Incident Response and Recovery**

**Preparing for Digital Security Incidents**:

1. **Incident Response Plan**: Draft a plan detailing response steps for various scenarios.
2. **Response Team**: Assign a dedicated team for incident response.
3. **Communication Plan**: Outline how to communicate internally and externally during incidents.

**Responding to and Recovering from Incidents**:

1. **Detection and Reporting**: Implement mechanisms for early detection and reporting.
2. **Containment and Eradication**: Isolate affected systems and remove threats.
3. **Recovery**: Restore systems from backups, ensuring no remnants of the threat remain.
4. **Post-Incident Analysis**: Review the incident to identify lessons learned and improve future responses.

*User Note*: This framework should be customized with specific actions, roles, and communication strategies relevant to your organization. Include templates for reporting and analysis to streamline the response and recovery process.

# **Digital Incident Report Form**

**[Organization Name] Digital Incident Report**

**Date of Incident:** [Date]

**Reported By:** [Name]

**1. Incident Details**

* **Description:** Briefly describe the nature of the incident.
* **Systems Affected:** List the systems or data compromised.

**2. Impact Assessment**

* **Operational Impact:** Describe how the incident has affected operations.
* **Data Impact:** Detail the type of data compromised, if any.

**3. Initial Response**

* **Actions Taken:** Summarize immediate steps taken to contain the incident.

**4. Further Action Required**

* **Recommendations:** Suggest further actions to prevent recurrence.

**Signature of Reporter:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Note for Users:** Adapt these templates to fit the specific needs and context of your organization. Consider adding specific examples or scenarios relevant to your operations for clarity.

# **Template for Partner Collaboration Agreement Including Digital Security Expectations**

**This Agreement** is made between [Organization Name] ("The Organization") and [Partner Name] ("The Partner") to collaborate on [Project/Initiative Name]. Both parties commit to upholding the highest standards of digital security throughout the collaboration.

**1. Collaboration Scope:** Details the purpose, goals, and activities covered by the partnership.

**2. Digital Security Standards:** Both parties agree to adhere to specified digital security protocols, including data encryption, secure data exchange methods, and regular security audits.

**3. Data Sharing and Confidentiality:** Outlines conditions under which data may be shared, including commitments to protect sensitive information and comply with applicable privacy laws.

**4. Incident Response:** Establishes a joint protocol for responding to digital security incidents, including notification procedures and remediation steps.

**5. Compliance and Legal Obligations:** Confirms that both parties will comply with relevant laws and regulations regarding digital security and data protection.

**6. Term and Termination:** Specify the agreement's duration and conditions under which it may be terminated.

**7. Amendments:** Procedure for making amendments to the agreement.

**Signatures:**

[Organization Name] Representative: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_

[Partner Name] Representative: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_

# **Social Media Security Protocols Guide for CSOs**

Introduction

* Overview of the importance of social media security.
* Common threats faced by CSOs on social media.

Securing Social Media Accounts

1. **Strong Passwords**: Guidance on creating robust passwords.
2. **Two-Factor Authentication (2FA)**: Steps to enable 2FA on major platforms.
3. **Reviewing Access Permissions**: Regular audits of account access.

Understanding Privacy Settings

1. **Platform-Specific Guides**: Tailored advice for Facebook, Twitter, Instagram, etc., focusing on privacy controls.
2. **Data Sharing**: Recommendations on limiting personal data shared online.

Recognizing and Responding to Threats

1. **Phishing Awareness**: Identifying and avoiding phishing attempts.
2. **Social Engineering Defense**: Strategies to recognize and protect against manipulation.
3. **Reporting and Blocking**: Procedures for reporting suspicious activities and blocking malicious entities.

Best Practices for Usage

1. **Content Management**: Guidelines on posting and sharing content securely.
2. **Public vs. Private Accounts**: Deciding which account settings are best for your CSO's needs.
3. **Regular Audits**: Scheduling periodic security checks.

User Note

This guide should be adapted based on the specific social media platforms your CSO uses and the unique threats in your region. Always stay updated with the latest security features offered by social media platforms.

This outline provides a framework for developing detailed content tailored to the needs of CSOs in Afghanistan, focusing on practical steps and user-friendly advice to enhance social media security.

# **Email Security Checklist**

Email is a common way for bad people to try to trick you or harm your computer. It's important to be careful when you're checking your emails. Here's a simple list to help you stay safe:

1. **Check Who Sent the Email**

* If you don't know the person who sent the email, be cautious.
* Look at the email address carefully. If it looks strange or different (like misspellings or odd numbers), it might not be safe.

2. **Think Before You Click**

* Don't click on links in emails unless you are sure they are safe. If you're not sure, you can type the website address into your browser yourself.
* Be careful with emails that ask you to click on a link to update your password or personal information. These could be tricks.

3. **Attachments Are Tricky**

* Only open attachments from people you trust. If you weren't expecting an attachment, it might be a good idea to ask the sender if they really sent it.
* Be extra careful with files that end in .exe, .zip, or .rar. These can harm your computer.

4. **Look Out for Strange Messages**

* Be wary of emails with bad spelling or grammar. Many tricky emails have mistakes.
* If an email asks for personal information like your password or bank details, do not reply. Real companies usually don't ask for this kind of information in an email.

5. **Use a Good Email Filter**

* Use an email service that checks your emails for bad things before you see them. This can help keep many dangerous emails away.

6. **Update Your Email Password Regularly**

* Change your email password sometimes. A good password is like a strong lock that keeps bad people out.
* Use a mix of letters, numbers, and symbols in your password. And don't use the same password for different accounts.

7. **Be Careful with Public Wi-Fi**

* When you're using public Wi-Fi, be extra careful. It's easier for bad people to see what you're doing. If you can, avoid checking your email when you're on public Wi-Fi.

8. **Two-Step Verification**

* If you can, turn on two-step verification for your email. This is like having a second lock on your door. Even if someone knows your password, they can't get in without the second step.

9. **Learn About Phishing**

* Phishing is when someone tries to trick you into giving them your personal information. Learn what these tricks look like so you can avoid them.

Remember, staying safe with email is mostly about being careful and thinking before you act. If something looks wrong, it's better to be safe and double-check.

# **Quick Cybersecurity Checkup Checklist**

This checklist is designed to help your organization perform a quick cybersecurity checkup to ensure you are following basic cybersecurity practices. Regular completion of this checklist can help safeguard your organization against common cyber threats.

General Security Practices

* **Passwords are strong and unique** for all accounts and systems.
* **Two-factor authentication (2FA)** is enabled for email, social media, and other critical accounts.
* **Software and systems** are up-to-date with the latest security patches installed.
* **Antivirus and anti-malware tools** are installed and updated on all devices.
* **Firewalls** are enabled on all devices and network equipment.

Data Protection

* **Sensitive data is encrypted** both in transit and at rest.
* **Backups of critical data** are regularly performed and tested for integrity.
* **Access to sensitive information** is restricted to authorized personnel only.

Email and Communication Security

* **Staff are aware of and can identify phishing attempts**.
* **Use of secure communication channels** for sharing sensitive information.

Network and Internet Security

* **Public Wi-Fi use** is minimized, and VPNs are used when accessing organizational resources remotely.
* **Network monitoring tools** are in place to detect and alert suspicious activities.

Device and Remote Work Security

* **Mobile devices accessing organizational data are secured** with passwords, encryption, and remote wipe capabilities.
* **Remote work policies** are followed, ensuring secure connections and practices.

Incident Response and Reporting

* **An incident response plan** is in place and known to all employees.
* **Employees know how to report cybersecurity incidents** or suspicious activities.

**User Notes**

* **Frequency**: Perform this checkup at least quarterly or after any significant change in your IT environment.
* **Documentation**: Keep a record of each checkup. Note any issues found and actions taken.
* **Follow-Up**: Address any unchecked items as soon as possible. Some items may require further investigation or external assistance.
* **Training**: Use the checklist as a training tool for new employees to familiarize them with your organization’s cybersecurity practices.
* **Updates**: As cybersecurity threats evolve, revisit and update this checklist to include new best practices and areas of concern.

This checklist is a starting point for maintaining your organization's cybersecurity health. Regular attention to these areas can significantly reduce your risk of falling victim to cyberattacks.

# **Resources**

**General Cybersecurity Toolkits & Guides**

* **Electronic Frontier Foundation (EFF) Surveillance Self-Defense:** Offers clear guides on a wide range of digital security topics, from basic device protection to combating targeted surveillance. [Visit EFF SSD](https://ssd.eff.org/)
* **Digital Security First Aid Kit:** Provides practical resources and advice in a friendly and accessible format, including guides and emergency contact lists for digital attacks. [Explore the First Aid Kit](https://securityplanner.org/)
* **Access Now Digital Security Helpline:** Offers free remote, expert advice for CSOs and human rights defenders worldwide facing digital threats. [Get Help from Access Now](https://www.accessnow.org/help/)

**CSO-Specific Focus**

* **The Defender's Protocol:** A holistic security protocol for human rights defenders, helping to understand risks and enhance physical, digital, and wellbeing security. [Read the Defender's Protocol](https://openbriefing.gitbook.io/defenders-protocol/)
* **Cybersecurity Handbook for Civil Society Organizations (National Democratic Institute):** A comprehensive resource covering risk assessment, policies, and practical security measures directly relevant to CSO work. [Access the Handbook](https://www.ndi.org/publications/cybersecurity-handbook-civil-society-organizations)
* **Defending Politically Vulnerable Organizations Online:** Highlights cybersecurity threats faced by media outlets, human rights groups, NGOs, and other politically vulnerable organizations, emphasizing the need for protection. [Read the CLTC Report](https://cltc.berkeley.edu/wp-content/uploads/2018/07/CLTC_Defending_PVOs.pdf)
* [**Citizen Clinic**](https://cltc.berkeley.edu/program/citizen-clinic/#:~:text=Citizen%20Clinic%20is%20empowering%20civil,they%20can%20drive%20social%20change.) is a public-interest cybersecurity clinic at the University of California, Berkeley. It trains students from various disciplines to help civil society organizations, such as journalists, human rights defenders, and social justice activists, to defend themselves against digital threats, such as cyberattacks, surveillance, harassment, and disinformation. Citizen Clinic aims to empower these organizations to use technology to fulfill their missions and drive social change.