Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Securing Access in a Volunteer-Based Organization

MANAGEMENT

FOREWORD

This document is an unclassified publication that has been issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, email, or phone our contact centre:

Contact Centre

cyber.gc.ca

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

EFFECTIVE DATE

This publication takes effect on January 14, 2022.

REVISION HISTORY

Revision	Amendments	Date
1	First release.	January 14, 2022

ISBN 978-0-660-41545-1
CAT D97-4/30-010-2022E-PDF

OVERVIEW

This document outlines common risks faced by volunteer-based organizations and recommends how to address these risks by adapting how people, processes, information, and technologies are managed. This document is intended for cyber security program owners, managers, and cyber security practitioners.

In this publication, we will focus on organizations that leverage a high number of volunteers. This could include museums, political parties, and electoral bodies, or any organization with a heavy reliance on volunteers. This represents additional challenges that could include a high turnover in volunteers and even volunteers with privileged access.

If your organization is based on a volunteer workforce (in whole or in part), you may face unique cyber security challenges. These challenges can arise if your environment includes a workforce that can change rapidly, expedite processes with reduced candidate vetting, and has limited budgets for solutions and expertise. If unaddressed, these factors can lead to risks that could leave your networks, systems, and information vulnerable to cyber threats.

TABLE OF CONTENTS

1 Introduction **5**

2 Managing People and Accounts **6**

2.1 Vetting and Reliability Verification 6

2.2 Cyber Security Training 7

2.3 Legal Considerations 7

2.4 Insider Threat 8

2.5 Account Lifecycle Management 9

2.6 Authentication 9

2.7 Providing and Revoking Access 10

3 Managing Processes **11**

3.1 Onboarding 11

3.2 Offboarding 11

4 Managing Technology **12**

4.1 Shared Equipment 12

4.2 Bring Your Own Device (BYOD) 13

4.3 Monitoring 14

5 Managing Information **15**

5.1 Information Handling 15

6 Supporting Content **16**

6.1 List of Abbreviations 16

6.2 Glossary 16

6.3 References 17

1 INTRODUCTION

This document outlines some of the factors that contribute to the cyber security risks volunteer-based organizations experience. To reduce these risks, we provide some actions your organization can take to ensure you can manage your people, accounts, processes, technology, and information with security in mind.

As a volunteer-based organization, you may face certain challenges that can contribute to higher levels of cyber security risks. Some of these factors include the following examples:

- You have **a limited IT budget**: With a limited budget, it is not reasonable to expect that all risks will be addressed. You should have a well-documented risk register (i.e. risk management tool) to prioritize risks. Follow the 80/20 rule to reduce 80% of the risks by addressing 20% of the known vulnerabilities.
- You may encounter issues with **account lifecycle management**: Your organization needs to review and confirm that all active user accounts are necessary and associated with volunteers who currently require access. Account access should be revoked when a volunteer is no longer working for your organization.
- You need to **quickly adapt to increased or reduced demand** in your workforce: You rely heavily on your volunteers, but you need the agility to ramp up or down quickly based on your workforce. In the cyber security context, this can mean that you need to rapidly activate and deactivate accounts, which can lead to risks caused by provisioning, human error, and account life cycle mismanagement.
- You may be at a higher risk of **insider threats**: High turnover rates and shortened or bypassed vetting processes can increase your risk of insider threats because it can be more difficult to identify volunteers with malicious intent. If your organization deals with highly sensitive information a more extensive vetting process may be necessary (e.g. police background checked).
- You may allow volunteers to **work with personal devices or shared equipment**: It may not be cost effective for your organization to give volunteers corporately owned devices or have equipment available for everyone. Users may share equipment or use personal devices; however, these options introduce additional risks that your organization should consider and evaluate.

2 MANAGING PEOPLE AND ACCOUNTS

There is always a level of risk associated with providing someone (i.e. employee or volunteer) access to your networks, systems, and information, regardless of how much vetting you perform. When dealing with limited resources (e.g. time and budget), you may need to accept additional risks to accommodate your rapidly changing workforce. This section covers some best practices that your organization can implement to reduce the risks associated with user accounts and access.

2.1 VETTING AND RELIABILITY VERIFICATION

Tailor your candidate vetting processes for the level of access each user requires. For example, you should conduct more thorough and rigorous vetting for a user who has access to sensitive information or privileged access to systems. Different vetting techniques provide different levels of security assurance and have varying costs (both monetary as well as the time required to complete).

Your candidate vetting process may include the following aspects:

1. **Resume verification** can help you identify employment gaps or issues (e.g. termination) that could signify risks.
2. A **criminal background check** can be performed quickly and be processed through a third-party partner. Performing a criminal background check provides valuable information at a low cost.
3. **Reference verification** is a step often included in the candidate selection processes and can help you gather feedback from the candidate’s previous managers or peers. Be cautious when validating references, as candidates do not usually include references who could provide negative feedback.
4. A **cyber security interview** can be performed to evaluate how comfortable the candidate is with cyber security best practices. This could be valuable if the candidate is to have privileged access.
5. A **security or reliability interview** performed by a security officer provides a deeper understanding of the risks related to a candidate. These interviews can be costly and time consuming. This interview is usually required when working with a public sector organization.

2.2 CYBER SECURITY TRAINING

All volunteers should be trained regardless of how long they are working for your organization. Training promotes security awareness and reduces the risks associated with user behaviour. Your organization should include the following practices in its cyber security training program:

- Provide mandatory training when onboarding volunteers and when there are changes to your policies and processes:
  - Address common threats to your organization, cyber security policies and processes, expected user behaviour, and incident response processes;
  - Include exercises that help users identify common threats such as phishing and social engineering attacks. Refer to *ITSAP.00.101 Don't Take the Bait: Recognize and Avoid Phishing Attacks* [1] for more information;
  - Inform your volunteers of your organization's password policy and provide tips on creating passphrases or complex passwords. Refer to *ITSAP.30.032 Best Practices for Passphrases and Passwords* [2] for more information;
- Provide refresher training courses routinely (e.g. annually) to keep volunteers up to date on your current security practices; and
- Tailor your training to address your organization's threat landscape and mitigation strategies.
  - Outline the threats that are specific to your organization to help volunteers understand why certain security controls are in place. Refer to *ITSM.10.093 Top 10 IT Security Actions: #6 Provide Tailored Cyber Security Training* [3] for further information.

2.3 LEGAL CONSIDERATIONS

Prior to granting access to your organization's systems, all volunteers should receive, read, and acknowledge their agreement to the standard organizational policies (e.g. code of conduct). Your organization should also implement an information management (IM) and IT acceptable use policy to cover how devices are monitored and the proper use of organizational assets and information.

All volunteers should receive an agreement that they acknowledge and sign when hired. This agreement should clarify how to handle organizational information and the consequences of any unauthorized sharing of that information.

Your organization should also evaluate the cost and benefits to having cyber security insurance to help protect systems and information. Understanding the policies behind your cyber security insurance is important when considering possible attacks that might not be covered under terms and conditions (e.g. a state sponsored threat).

2.4 INSIDER THREAT

An insider threat is anyone who has knowledge of, or access to, your organization's infrastructure and information and who uses, either knowingly or inadvertently, the infrastructure or information to cause harm. Insider threats can put your organization's volunteers, customers, assets, reputation, and interests at risk.

Someone could inadvertently cause harm to the organization through the following actions:

- Misplacing a mobile device or removable media;
- Granting other people access to sensitive information; and
- Mishandling sensitive information.

Someone with malicious intent could carry out the following actions:

- Expropriate information and documentation;
- Modify or delete content;
- Modify accounts to grant access to unvetted users;
- Modify the sensitivity of a document to make it accessible to more people; and
- Perform a ransomware attack by encrypting documents and asking for payment in exchange of decrypting documents.

Interviews, security clearances, background checks, and reference verifications are steps that help confirm the trustworthiness of volunteers. When your workforce needs to be ramped up quickly, you might not have time for thorough vetting processes. Your organization might need to accept the risks associated with a partial verification or no verification at all. For more information on insider threats, see *ITSAP.10.003 How to Protect Your Organization from Insider Threats* [6].

2.5 ACCOUNT LIFECYCLE MANAGEMENT

Your organization may need to work with both short-term and long-term engagements. Short-term engagements can be a challenge; the IT overhead is increased, the risks of mishandling an account are greater, and the vetting and onboarding processes need to be streamlined.

Your onboarding and offboarding processes should include the following security measures:

- Apply the principle of least privilege to ensure that users only have access to the systems and information they need to carry out their work functions;
- Disable accounts when they are no longer required;
- Implement and enforce a strong password policy;
  - Refer to *ITSAP.30.032* [2] for more information;
- Use account creation templates that have the correct security policies applied when creating new accounts;
  - Set expiration dates on accounts based on the frequency of access reviews;
  - Consider using automation to help manage batched account creations;
- Set expiration dates to disable accounts based on volunteers' schedules;
- Restrict logon hours for users' accounts based on volunteers' schedules;
- Review accounts periodically and acquire manager approval (i.e. the accountable manager confirms validity of accounts and communicates back on accounts that should be modified or disabled); and
- Select a vendor in Canada for cloud account management and be familiar with their conditional access policies.

2.6 AUTHENTICATION

In securing accounts and devices, it is important to use methods of authentication to keep sensitive information secure. Implementing the following best practices will help mitigate the risks associated with passwords:

- Establish a password policy that includes the following aspects:
  - Requires a minimum length of 12 or more characters for passwords;
  - Encourages the use of passphrases of at least 15 characters;
  - Enforces a minimum level of complexity (e.g. special characters, numbers, and letters used);
- Use shared accounts **only if** no other options are available;
- Enable multi-factor authentication (MFA) for all accounts (e.g. general user accounts, administrative accounts, and privileged access accounts) to add extra security measures where possible; and
- Implement an account lockout policy.
  - Lock accounts after 3 to 5 attempts.
  - Enable ability to unlock accounts only by administration.

See *ITSAP.30.030 Secure Your Accounts with Multi-Factor Authentication* [4] and *ITSP.30.031 v3 User Authentication Guidance for Information Technology Systems* [5] for more information.

2.7 PROVIDING AND REVOKING ACCESS

Securing access for information is important in keeping the sensitive data of your organization secure. If many users share similar roles and need similar access, managing access can be easier by practicing the following:

- Create groups according to your organization’s security needs and access requirements;
  - Users with limited and read only access;
  - Users with requirements for additional access (e.g. modify, move);
  - IT personnel with requirements around supporting the organization’s workforce;
  - Special access users with requirements to access limited audience documents;
- Leverage folder structures that align with security needs of various groups of users based on the level of access required;
- Grant access to the required groups (in lieu of each individual) when configuring access;
- Add users to groups that match each individual role and access level when onboarding;
- Remove accounts from groups when offboarding to revoke all access;
- Restrict the ability to view memberships and add and remove users from groups to privileged account users;
- Reserve the ability to change group access permissions to a small group of administrators; and
- Use a Cloud Access Security Broker (CASB) solution for data loss prevention and IM to ensure data integrity.

3 MANAGING PROCESSES

This section recommends best practices for mitigation risks associated with your onboarding and offboarding processes. Your organization needs the agility to provide all required resources quickly and efficiently to volunteers. However, this quick transition can lead to human errors, typographical mistakes, missed steps, or access control errors. Below are recommendations to help mitigate risks associated with processes.

3.1 ONBOARDING

Onboarding can be a lengthy process that volunteer-based organizations need to streamline. Your onboarding process would also ideally allow for the batch creation of accounts when a high number of volunteers are required in a short amount of time. To keep the risk as low as possible while meeting this requirement, consider the following actions:

- Use automated tools or scripting to expedite repetitive tasks;
- Use templates with tested security settings and policies to meet security requirements for new accounts;
  - Changes (or attempts to change) to this template should be restricted and logged to mitigate unnecessary access to new users;
- Communicate default passwords safely to users (e.g. communicated in person, over the phone, or in secure messaging) and require a password change at first login; and
- Train new volunteers as early as possible (e.g. in-classroom, online training, or written materials).
  - Online training with a “quiz” functionality can help make sure that the key elements of the training were retained.

3.2 OFFBOARDING

Offboarding is a complex process. There are many aspects of the process that you need to consider, such as decentralized authentication, sessions that are considered authenticated with unexpired tokens, on-premises accounts (e.g. Active Directory [AD]), cloud accounts (e.g. Office 365, Azure AD), federated accounts (e.g. AD Federation Services [ADFS]), and third-party accounts (e.g. software as a service [SaaS] with separate authentication).

A good offboarding process needs to minimize the risk of human error and allow access to be fully revoked if a step was not completed properly.

A recommended offboarding process should include the following elements:

- Automate processes as much as possible;
- Disable accounts;
- Revoke certificates and tokens from accounts;
- Revoke authentication tokens from cloud services;
- Disable access to devices that have access through bring-your-own-device (BYOD) capabilities; and
- Wipe organizational data from BYODs.

4 MANAGING TECHNOLOGY

This section recommends best practices that you can apply to mitigate the risks associated with your technology. Using corporately owned equipment ensures that you have more control over the security of equipment and devices. While it is ideal to provide corporately owned equipment to everyone in your organization, it might not be possible. Offering shared equipment or BYOD capabilities and working through cloud services might be more manageable, but you should ensure that you take steps to mitigate the risks associated with those options. It is possible to provide BYOD capabilities to specific users or groups without necessarily allowing it to all users.

When deploying mobile devices and equipment in your organization, you should consider different deployment models. With this technology, managing risk depends partly on volunteer cooperation (i.e. willingness to allow use restrictions, monitoring, and security access by the organization) and partly on the inherent risks and vulnerabilities in the types of devices included. To select a deployment model that best balances these elements for your organization, consider user experience, privacy, and security requirements. For more information, see *ITSAP.70.002 Security Considerations for Mobile Device Deployments* [7].

Use mobile device management (MDM) through a trusted vendor to manage administration and monitoring on devices. MDM is used to implement a checklist of automatic security measures that can include smooth onboarding and offboarding processes for all equipment.

4.1 SHARED EQUIPMENT

Shared equipment can be convenient and help keep costs down, but it also comes at the cost of additional risk. One user clicking a malicious email and infecting the computer has the potential to impact all users who share the same device. Some cloud storage solutions for example will make available files offline by copying those files to the local hard drive. Should multiple users use the same computer and also have offline copies of their files, each user's files could be affected.

If volunteers use shared devices, the following additional security measures should be applied to the devices:

- Install and frequently update anti-virus and anti-malware software;
- Disable administrative rights on users' accounts and devices unless it is necessary;
- Allow separate accounts to be accessed through shared devices;
- Monitor and restrict internet browsing if use is required, and block otherwise; and
- Use virtual desktop infrastructure (VDI) to mitigate the risks associated with volunteers using desktops, if possible.
  - Refer to ITSAP.70.111 *Using Virtual Desktop At-Home and In-Office* [8] for more details on VDI.

4.2 BRING YOUR OWN DEVICE (BYOD)

Providing BYOD capabilities can be hugely beneficial to an organization. Not needing to procure and maintain devices reduces cost. Such capabilities can allow users to use personal computers, tablets, or mobile devices to access organizational data. Your organization can implement policies to protect as much of your data that resides on personal devices as possible, but the devices themselves remain managed by their owners.

The convenience and cost savings of such capabilities can outweigh the risks. This can put IT departments in a situation where it is not “if” this should be implemented but “how” can it be implemented safely.

When considering a BYOD option, consider the following security measures:

- **Application protection policy**
  - Prevent organization contacts from being accessed by applications not protected by an application protection policy;
  - Only allow installation of applications from trusted sources; and
  - Isolate BYOD devices on a different network or subnet if they are required to connect to the business network. Leverage firewalls to filter what connections are allowed to and from the BYOD network will help reduce the risk associated with personal devices on an organization network.
- **Offboarding process**
  - Include the necessary steps to disconnect any BYOD devices, and revoke authentication tokens, and wipe organization data from devices when offboarding.
- **Logging and auditing controls**
  - Log all actions performed by BYOD devices; and
  - Use a CASB to register and monitor devices.
- **Device compliance**
  - Implement a conditional access policy, prior to granting access, to make sure personal devices are not compromised;
  - Ensure devices are connected with user accounts and issued certificates;
  - Verify the device is not jail broken (iOS), rooted (Android), or otherwise compromised;
  - Configure an application protection policy for BYOD devices to enforce additional security requirements before company data can be accessed (e.g. PIN, password, biometric); and
  - Permit access only to devices that meet the compliance requirements (e.g. not rooted or jailbroken, running a recent version of the operating system, an approved device manufacturer).

4.3 MONITORING

Monitoring and logging activity is necessary to report incidents and respond effectively. The following areas should be logged and kept at least 90 days or longer, if possible:

- User logins (e.g. successful or failed);
- User modifications (e.g. create, delete, disable, password change);
- Documents accessed and actions made (e.g. create, copy, move, download, delete);
- Security group modifications (e.g. added and removed users);
  - Adding a user to a group and adding a group to a group might be logged differently (e.g. different event ID);
- Privileged access logins and logouts; and
  - Any changes applied during a privileged session;
- Backups performed (e.g. errors reported).

Your organization’s logs should display accurate time stamps and usernames. The logs should also be monitored. If possible, use a security information and event management (SIEM) system or security operations centre (SOC) to monitor logs and events around the clock.

5 MANAGING INFORMATION

5.1 INFORMATION HANDLING

To secure your organization’s data when being handled by volunteers and technologies, all documents should be marked with their appropriate sensitivity level. You should require and enforce marking information. To help with this process, create simple and clear guidelines to ensure that all volunteers know how to mark information adequately.

An example of a dissemination model is the Traffic Light Protocol (TLP), which is a model that was created by the UK Government’s National Infrastructure Security Coordination Centre. You can use this model to identify sensitive information and label it with designations to ensure that the information is shared appropriately when sharing is required. The TLP consists of four designations:

- **White**: Distribution is not restricted, and the information can be shared with anyone;
- **Green**: Distribution stays within the organization;
- **Amber**: Distribution stays within the organization and is restricted to a need-to-know basis only; and
- **Red**: Distribution is limited to meeting attendees and conversation participants.

For more information on the TLP, refer to *Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance* [9].

Once information has been marked, technology can be leveraged to ensure that information doesn’t go beyond boundaries set by the organization. Firewalls, data loss prevention technology, cloud access security broker, and other technologies can be used to prevent the mishandling of information (accidental or deliberate). Having your information marked will help make the technology solution more effective.

6 SUPPORTING CONTENT

6.1 LIST OF ABBREVIATIONS

Term	Definition
AD	Active Directory
ADFS	Active Directory Federation Services
BYOD	Bring Your Own Device
CASB	Cloud Access Security Broker
iOS	iPhone Operating System
IT	Information Technology
MFA	Multi-Factor Authentication
PIN	Personal Identification Number
SaaS	Software as a Service
SIEM	Security Information and Event Management
SOC	Security Operations Centre
TLP	Traffic Light Protocol
VDI	Virtual Desktop Infrastructure

6.2 GLOSSARY

Term	Definition
Administrative privileges	The permissions that allow a user to perform certain functions on a system or network, such as installing software and changing configuration settings.
Biometric	Biometrics refers to the measurement and use of your unique body characteristics (e.g. fingerprints, retinas, facial structure, speech, or vein patterns).
BYOD	Employees use their own devices for business purposes, and organizations may choose to cover some of the costs associated with the devices. However, because your organization does not own the device, it has little control over the security controls implemented on the device.
CASB	A cloud access security broker is a cloud based software that monitors activities and enforces security measures between accounts and applications.
Classified information	A Government of Canada label for specific types of sensitive data that, if compromised, could cause harm to the national interest (e.g. national defence, relationships with other countries, economic interests).
Encryption	Converting information from one form to another to hide its content and prevent unauthorized access.
Insider threat	Anyone who has knowledge of or access to your organization’s infrastructure and information and who uses, either knowingly or inadvertently, the infrastructure or information to cause harm.
Jailbreak	The process of exploiting a device to remove limitations imposed by the manufacturer. Also referred to as rooting on Android devices running the Android operating system.

Term	Definition
Least privilege	The principle of giving an individual only the set of privileges that are essential to performing authorized tasks. This principle limits the damage that can result from the accidental, incorrect, or unauthorized use of an information system.
Phishing	An attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing, a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.
Ransomware	A type of malware that denies a user's access to a system or data until a sum of money is paid.
Risk	In the cyber security context, the likelihood and the impact of a threat using a vulnerability to access an asset.
SIEM	SIEM is a product or service that gathers large quantities of security logs and performs automated aggregation, normalization, event reporting, incident management and other security functionality. User behaviour analysis can also be functionality provided by a SIEM.
SOC	A SOC is usually comprised of a team of security analysts reviewing logs and events around the clock, performing real time evaluation of events, perform deep dives when necessary and provide incident reporting and response.
Threat	Any potential event or act (deliberate or accidental) or natural hazard that could compromise IT assets and information.
VDI	Using technology to host virtual desktop environments on organizationally owned or personal devices. This technology enables users to access their workstations through a virtual session connected to the device.
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited by a threat actor to adversely affect an organization's assets or operations.

6.3 REFERENCES

Number	Reference
1	Canadian Centre for Cyber Security. *ITSAP.00.101 Don't Take the Bait: Recognize and Avoid Phishing Attacks*. April 2020.
2	Canadian Centre for Cyber Security. *ITSAP.30.032 Best Practices for Passphrases and Passwords*. September 2019.
3	Canadian Centre for Cyber Security. *ITSM.10.093 Top 10 IT Security Actions: #6 Provide Tailored Cyber Security Training*. February 2020.
4	Canadian Centre for Cyber Security. *ITSAP.30.030 Secure Your Accounts with Multi-Factor Authentication*. June 2020.
5	Canadian Centre for Cyber Security. *ITSP.30.031 v3 User Authentication Guidance for Information Technology Systems*. April 2018.
6	Canadian Centre for Cyber Security. *ITSAP.10.003 How to Protect Your Organization From Insider Threats*. February 2020.
7	Canadian Centre for Cyber Security. *ITSAP.70.002 Security Consideration for Mobile Deployments*. June 2020.
8	Canadian Centre for Cyber Security. *ITSAP.70.111 Using Virtual Desktop At-Home and In-Office*. August 2020.
9	FIRST. *Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance v.1*.