Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

Wi-Fi Security

PRACTITIONER

TLP:WHITE

Canada

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 March 31, 2022.

REVISION HISTORY

Revision	Amendments	Date
1	First release.	March 31, 2022

ISBN 978-0-660-42809-3
CAT D97-3/80-002-2022E-PDF

OVERVIEW

Wi-Fi is everywhere: in your local coffee shop, in your home, and at work. As organizations rely more on Wi-Fi, attention to fixing the security landscape of wireless networks must also increase to reduce the risks cyber threats. This document is intended for organizations of all sizes, both public and private, using Wi-Fi.

This document provides awareness of the vulnerabilities that exist within networks that introduce or currently use Wi-Fi. It is important to consider Wi-Fi security as an integral part of network and infrastructure security as it is used to carry out critical tasks that often include sensitive and confidential information (e.g. trade secrets, personal information [PI], and copyrighted material). A network is only as secure as its weakest link and Wi-Fi is an easy target for threat actors to take advantage of.

In this document, you will find sections corresponding to the Cyber Centre's recommended policies, technical controls, and security measures as well as additional considerations to ensure network-wide security.

TABLE OF CONTENTS

1 WI-FI THREAT AWARENESS

Being aware, identifying the risks, and addressing known vulnerabilities associated with poorly secured Wi-Fi are the first steps in securing your network. This section presents common risks with wireless networking and provides information on identifying organizational changes that can be applied to reduce the risks.

1.1 NETWORK ATTACK AWARENESS

When securing Wi-Fi, it is important to recognize the following threats to your wireless network and how they can be mitigated.

Unpatched firmware: Unpatched firmware can leave your wireless network vulnerable to security breaches. Threat actors may take advantage of firmware that is not updated with the newest version. Ensure your organization has a patching policy in place that schedules regular updates for all device firmware, including access points and controllers.

Insecure defaults: Many wireless devices come with insecure defaults, such as known usernames and passwords, bridges connecting network ports or virtual local area networks (VLANs) together, firewall rules that allow everything through, and client isolation on Access Points turned off. Changing your default username and passwords on your Wi-Fi network to strong and unique keys, along with hardening each network device's settings, are very important steps to mitigate weaknesses.

Shared networks: Any division of duties or roles (e.g. staff and guests) on the network should have separated network spaces controlled with client isolation, VLANs and switches, and firewall rules. Segment your network into security zones to mitigate these risks and reduce the attack surface for cyber threat actors.

After separating your users into different network security zones, you should separate wired and wireless networks into different segments as well for each division. This will prevent attacks on your wireless network from obtaining direct access to wired devices and clients, assuming that your firewall and network hardware are configured to block such access. For example, if you have a guest and a staff network segregated from one another, you should then split each of those zones into wireless and wired zones. This would result in four zones total, two Wi-Fi and two wired zones.

Internet of Things (IoT) devices: IoT devices are commonly used in small office home office (SOHO) and small medium business (SMB) organizations. These devices carry significant security risks due to poor security design, and lack of software or firmware updates. If possible, these devices should be avoided, or segregated onto a separate network.

Wardriving or parking lot attack: Wardriving is the practice of creating a mobile reconnaissance centre (and sometimes an attack centre). This could be a van outfitted with wireless analysis tools (e.g. spectrum analyzer, powerful or highly-directional receiving antennas, mobile computing equipment) or it could be as simple as a single laptop, cell phone, or tablet. Not all wardriving has malicious intent and is often used as a form of research to identify common risk factors for individuals and organizations. Parking lot attacks are more targeted and generally involve more than simply listening to wireless signals. The targeted attack area could be outside conventional security controls such as gates, secured doors, or security camera systems. Signal strength should be limited to avoid those sitting, driving, or walking nearby from launching wireless attacks on your network.

Device theft: Wi-Fi devices or modules are not always restricted to their locations as they are designed to be mobile and can be easy to pick up. This creates additional risk with respect to the theft of those devices. A smart lightbulb, for example, can often be found in a public location and may contain access credentials to the wireless network. Unrestricted access to the lightbulb may allow a threat actor access to these credentials, which can later be used to connect to the wireless network. Some devices such as phones or tablets can contain sensitive data (e.g. sensitive personal information) on them and are much easier to steal than a desktop computer. No easily stolen device with sensitive information or access credentials should be left in an untrusted location, unlocked, or not physically secured.

Rogue access points: These are common in public Wi-Fi environments such as coffee shops, restaurants, airports, and public Wi-Fi locations. Attackers will often deploy devices that pretend to be a trusted network for the physical area, therefore when you look for available networks (or your device automatically does) you may be authenticating against a malicious rogue access point. Always ensure you are connecting to the correct Wi-Fi network and use encrypted communication techniques.

Another common tactic is corporate Wi-Fi networks being spoofed. A guest with access to the organization can spoof the network in a nearby location by deploying a malicious access point.

These attacks can lead to data leaks and unauthorized access.

Weak authentication: Using pre-shared key (PSK) over enterprise is not recommended for any organization as it does not authenticate individuals as everyone shares the same passphrase. You cannot determine who used the passphrase or if the access is legitimate. Implementing a password policy when using Wi-Fi Protected Access (WPA) enterprise is very important to ensure that passwords are long and complex enough to make certain they are not easily compromised.

Weak encryption algorithms: Using weak or outdated encryption algorithms can offer threat actors an easy way to compromise your wireless network. The attacker can use various wireless tools to compromise the system and does not need to physically plug anything into the network to exploit it. Please refer to *ITSP.40.062 Guidance on Securely Configuring Network Protocols* [1] and *ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information* [2] for recommended algorithms to use.

1.2 BREACH EXAMPLES

In 2015, a zero-day (e.g. computer or software vulnerability with no existing available patch) for ANTLabs InnGate routers was discovered, CVE-2015-0932. While quickly patched once discovered, it caused a breach of 277 different hotels, convention centres, and data centres. This router was typically deployed in networks used in many hotels and other networks that include guests.

This zero-day allowed attackers to take control of the router and install malware, launching attacks against connected systems, and completely controlling the Wi-Fi and wired networks that guests connected to.

Another example of a breach occurred in 2015. WeWork, a commercial real estate company, had their Wi-Fi network compromised due to it having poor security for their building tenants. Anyone could pay $25 to access a boardroom and the Wi-Fi network, perform a network scan and obtain sensitive information from the many businesses that use the network. This issue wasn't confined to one building, as many of WeWork's buildings also contained the same PSK. This resulted in a

massive security incident affecting personal documents such as drivers' licenses, passports, job applications, bank account credentials, contracts health records, and more. [3]

During 2021, from January to June, Kaspersky reported that there were 1.51 billion breaches of IoT devices which had increased from 639 million in 2020. Typically, these attacks involved the use of the telnet protocol which allows remote administration on the command line interface. These attacks are carried out to perform distributed denial of service (DDoS) attacks, as well as cryptocurrency mining or to pivot to other more sought-after targets on the network. The global pandemic has caused increased use and attention to IoT devices. [4]

In another case, Eduroam, a free Wi-Fi network used by a multitude of universities across Europe was found to have a misconfiguration with the Extensible Authentication Protocol (EAP) that could lead to an 'Evil Twin' attack where the attackers simulate the network to trick devices into connecting to the wrong network. Given that some OS's do not validate the certificate when connecting to a system, this opens up the possibility of stealing credentials used for Wi-Fi connections. In this configuration, Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPV2) should have been used rather than the less secure Password Authentication Protocol (PAP). [5]

2 BEST PRACTICES

2.1 DATA STRUCTURES

Structure-based approaches to security ensure that resources are setup in a way that allows easy provisioning, maintenance, and security uptake while ensuring sensitive data is only reachable by those who require it. Without structure, your data can be placed anywhere and there is no discerning between data that contains sensitive information and public data.

2.1.1 LIMITING INFORMATION AVAILABLE

Sensitive information (e.g. business proprietary, classified, confidential, or personal data) should not be transmitted on open networks without additional encryption controls. Threat actors can sit nearby and intercept the network communications. It is important to implement least privilege ensuring each associate in an organization only has access to the files and resources they require to do their job.

For more details on limiting sensitive information, refer to *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [6].

2.1.2 STRUCTURING CLASSES OF DATA

Structuring classes of data ensures that sensitive data never leaves the area where it is protected and limits the damage of a data or privacy breach. Data should be structed in a way that conforms to the organization's security and privacy needs and keeps personal and confidential information secure. An example method of structuring these classes is provided below.

Class 1: Public data

This class of data is used to define data that is accessible and available to the public. No harm would be done to the business, clients, staff, or vendors with this data being handled internally and externally. Some examples of public data include: an organization's public webpages, brochures, and business cards.

Class 2: Internal-only data

This type of data is only meant to be used inside the organization with authorized personnel. Internal-only data contains slightly sensitive information about the organization's operations, policies, or business plans. Some examples are internal memos and business-related emails. If this data were to get out to those without authorization it could pose minimal harm to the business.

Class 3: Confidential data

This data is limited to a specific group within the organization who hold a special clearance or clear permissions to use and access this data. Confidential data may contain PI that would cause great harm to the organization, individuals, and parties involved if compromised. Typically, this data is protected under the provisions of the federal and private sector privacy legislation (i.e. the privacy act and the Personal Information Protection and Electronic Documents Act [PIPEDA]), as well as by the Payment Card Industry Data Security Standard (PCI DSS) or is regulated under the Investment Industry Regulatory Organization of Canada (IIROC) or the Mutual Fund Dealers Association (MFDA) of Canada. Examples of this data include proprietary business data, research data, source code to software, and other PI.

2.1.3 STRUCTURING YOUR WI-FI AND WIRED NETWORKS

Wi-Fi devices allow you to have multiple service set identifiers (SSIDs) configured. Each SSID should have its own VLAN to limit access to inner zones of the network, along with enhanced security measures (e.g. structuring your network). Beware of default settings that allow all traffic to flow between SSIDs or VLANs. Please review the SSIDs and VLANs technical controls subsection 2.3.2 for more information.

If your organization provides a guest Wi-Fi network for visitors to use while at your establishment, limit the period of time that the guest password can be used (e.g. password expires daily or offer guest passes) to ensure only current guests can access your network.

For additional information on network zoning, refer to *ITSG-38 Network Security Zoning - Design Considerations for Placement of Services within Zones* [7]**.**

2.2 POLICY BASED

Written policy must fully reflect your stance on security and privacy. Technical controls implement what is published in the written policy. Technical controls without written policy may not withstand legal challenges. Below you will find various policies that can influence the security of your Wi-Fi network and business.

2.2.1 ACCEPTABLE USE POLICY

This type of policy is used to clarify what a service, network, system, or website may be used for. Its main purpose is to reduce legal liability and give users a clear understanding of how something can and cannot be used. This policy should include the permitted classes of web access. Some categories of websites can draw attention to your organization, increasing the overall risk. This policy should be combined with technical controls that help to enforce the policy (e.g. a web filtering service on a firewall).

2.2.2 BRING YOUR OWN DEVICE (BYOD) POLICY

If your organization allows the BYOD model, it is recommended you implement a BYOD policy. A BYOD policy should enforce additional restrictions that apply to devices used in a BYOD environment and it must be both enforceable and auditable. Anything that is not enforceable or auditable via technical controls, should be considered as risks to the organization. The BYOD policy should define:

- the application and permission vetting process for apps and data;
- the minimum-security precautions to take;
- the classes of data that are stored on a device;
- the intention of providing this method of connection to the organization;
- the proper way to discard, copy, and sync data;
- the requirements surrounding the method and type of device or application encryption; and
- the best practices deemed necessary for secure operations.

2.2.3 ENCRYPTION AND DATA SECURITY POLICY

The encryption and data security policy should define what data should be encrypted, what encryption algorithms are acceptable, and the parameters that are considered "secure" for the organization. It should cover portable media encryption, data at rest, and data in transit. This policy should also define a standard depending on the class of data in question.

2.2.4 DATA GOVERNANCE POLICY

The data governance policy should define the retention of data, the acceptable destruction methods, and the general lifecycle of data based on the class. It should also define data residency requirements and the controls in place.

2.2.5 PASSWORD POLICY

A password policy should define the requirements for secure and acceptable password use for the organization. For low sensitivity environments, the minimal best practices might be considered enough. For high sensitivity environments (e.g. financial and healthcare) the requirements should include high security measures. This policy should also discuss who can reset or change a password and how credentials can be securely stored. The Cyber Centre does not typically recommend using password expiration and password re-use.

For further information on best practices for passwords and passphrases, refer to *ITSAP.30.032 Best Practices for Passphrases and Passwords* [8].

2.2.6 PATCHING POLICY

The patching policy defines what equipment is patched and how often it is patched in the environment. Examples of systems that should be included in the patching policy are mobile devices, computer operating systems (OSs), applications, anti-malware or anti-phishing systems, and network equipment. The patching policy should include schedules for regular updates on all device firmware, access points, and controllers. The policy should define the authorized personnel who can perform the patches, the back-out plan if the updates fail, and who needs to be notified of the failed update (within the specified time).

2.2.7 PUBLIC WI-FI POLICY

The public Wi-Fi policy should have a dedicated policy or a section within another policy (e.g. an IT and network communication policy) that defines the appropriate use of public Wi-Fi networks (e.g. a coffee shop, hotel, or unmanaged network). This policy may include requirements to encrypt all data in motion, limit access to confidential classes of data, or follow precautions to prevent threat actors from obtaining sensitive organizational data.

2.3 TECHNICAL CONTROL BASED

Technical controls should be enforced to prevent security incidents and ensure data integrity through safe and secure access. Without technical controls, users' device data can be accidentally or maliciously intercepted, falsified, or compromised.

2.3.1 WI-FI ENCRYPTION AND PSK VERSUS EAP

Encryption

When choosing a Wi-Fi encryption method, you should use the one that is compatible with all your devices and network equipment.

Wired Equivalent Privacy (WEP): WEP can be easily compromised. WEP uses Rivest Cipher 4 (RC4) (i.e. a stream cipher algorithm) for confidentiality with a cyclic redundancy check (CRC32) (i.e. a checksum algorithm) for integrity.

WPA 1: A fairly strong encryption algorithm that uses RC4 with Temporal Key Integrity Protocol (TKIP) (i.e. an encryption protocol). WPA1 is not considered a secure enough encryption method for businesses handling sensitive information and should be avoided.

WPA2: A strong form of Wi-Fi encryption that is widely used across networks. Wi-Fi Protected Setup (WPS) should be avoided when using WPA2 for improving security. WPA2 uses 128bit Advanced Encryption Standard (AES) for encryption and Cipher Block Chaining Message Authentication Code Protocol (CCMP) to provide enhanced protection.

WPA3: The newest and most secure form of Wi-Fi encryption that uses 192bit AES in enterprise mode and 128bit in personal mode. If available, this should be used for all new deployments.

PSK versus EAP

PSK is the most widely used method to secure personal or SMB Wi-Fi networks. However, while PSK is very easy to implement, it is not recommended for business use of any kind, due to its lack of identity management and audit capabilities. PSK uses a passphrase to secure the wireless network and encrypt traffic. This method provides easy usability and setup with minimal support needed. However, once you give the password to someone the only way to lock them out is by changing the PSK, which will impact users' connectivity until the new passphrase is entered. All devices, including non-user devices such as wireless printers, would need to be updated with the new password or passphrase. There are alternatives for small businesses such as the Lightweight Extensible Authentication Protocol (LEAP), and Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol (PEAP-MS-CHAP). For large organizations, Extensible Authentication Protocol Transport Layer Security (EAP-TLS) is the most secure protocol you can implement. If PSK must be used, then separating guests, staff, information technology (IT) equipment and IoT into different SSID with VLANs and network segments with unique passphrases is crucial.

EAP is commonly used in medium to large organizations for wireless connectivity. This method allows the use of a username and password to authenticate each device as well as Transport Layer Security (TLS) based machine certificates. The most secure practice would be to use TLS certificates alongside EAP. This would allow you to individually disable a device's access to gain better visibility on who is using the Wi-Fi network. This method makes it more difficult for attackers to breach the network. Using Single-Sign On (SSO) with PEAP-MSCHAPV2 adds additional convenience by authenticating against a directory and reducing the number of logins users must remember. PEAP-MSCHAPV2 is a PEAP that allows users to enter in credentials which are authenticated by the Remote Authentication Dial-In User Service (RADIUS) server, inside of the EAP encrypted tunnel.

2.3.2 VLANS AND SSIDS

SSIDs are what most call the "Wi-Fi name" or "network name". They allow you to see and identify the Wi-Fi network you would like to connect to. Never put PI or confidential data in a SSID. For personal or small businesses, it is common to have one or two SSIDs being used (e.g. the employee network and a guest network).

VLANs allow virtual networks within the same physical infrastructure. Most managed switches and firewalls support the establishment and use of VLANs. You should use VLANs combined with SSIDs to create separate security zones within your network.

Separate wireless traffic from wired traffic by using a separate VLAN from all wired traffic to configure the SSID appropriately. Guest access should be separated with a restricted VLAN. All access points (APs) and SSIDs should have the option to turn on client isolation to prevent clients from talking directly to each other. Other devices, such as printers and IoT devices may not support WPA-EAP due to cost constraints, and should be placed on a separate, secure network that is isolated from the employee and guest networks. Do not let users access these networks and ensure they are locked down with a very strong password.

2.3.3 RADIUS

RADIUS works with EAP to create a secure authentication system that uses a RADIUS server from an AP or an AP controller. You must ensure the RADIUS server is using a secure secret for devices to connect and authenticate with. The secret is equivalent to a passphrase. Software on the APs, the AP controller, and the RADIUS server must be kept up to date and accounts managed closely.

Many RADIUS servers also connect to a directory for SSO authentication, typically by the active directory (AD) or an online cloud directory service.

2.3.4 DIRECTORY SECURITY

While the Wi-Fi APs, controller, and the RADIUS server are important, the directory validates credentials. It is important to use role-based access control (RBAC) and ensure physical and cyber security policies are in effect to secure the directory service. Typically, AD is used as the directory to authenticate users using SSO. The entirety of the directory server must be secure including the OS, applications, services, accounts, permissions, firmware, and hardware.

2.3.5 VIRTUAL PRIVATE NETWORKS (VPNS)

Public VPNs: These are typically used for protecting privacy of individuals or hiding point-of-origin in a public Wi-Fi network and should never be used for business connections. It can be challenging to know which vendors are reliable since you may not have the resources to investigate the security or infrastructure of a public service and often these services are run from servers located in countries that do not have strict privacy and data protection laws. Public VPN providers may also not vet technical staff who have access to both the unencrypted data as well as the customer identification and payment information.

Corporate VPNs: A corporate VPN is recommended when communicating to corporate resources over an unmanaged network (e.g. guest networks or public Wi-Fi). Corporate VPNs allow your device to create an encrypted tunnel to the corporate network and secure the data in transit. Even if an attacker is listening on the network, they will be unable to understand the data traversing as it is sent in an encrypted tunnel.

2.3.6 WPS

WPS makes it easier to connect to a network. Typically, this feature is found on SOHO equipment and allows pressing a physical button on the wireless access point to connect without typing in a password. This feature is only available on WPA encrypted networks. Modern versions of this feature allow entering a 6-digit pin, which inherently bypasses the password requirements for connecting to the wireless network. This feature should be disabled completely on any wireless equipment for business use as it is not secure.

2.3.7 ENDPOINT SECURITY

Any entry point into a wireless network is a potential attack vector. Ensuring that every endpoint device is secure helps mitigate the risk. Mobile device management (MDM) software can be applied as a technical control to identify users of mobile devices and to easily configure and push Wi-Fi, VPN, and authentication token configurations to devices.

For recommendations on general endpoint security please refer to *ITSP.70.012 Guidance for Hardening Microsoft Windows 10 Enterprise* [9].

For more information on general mobile security refer to *ITSAP.00.001 Using Your Mobile Device Securely* [10].

Securing your BYOD devices for the organization with both policy and technical controls helps ensure that your Wi-Fi is secure.

2.3.8 PHYSICAL SECURITY

Physical security is just as important as cyber security. Physical security reduces the chances someone physically resetting devices and connecting with default credentials, connecting into the wired network of the wireless device, or connecting to the wireless equipment and stealing credentials. If a device is factory reset, it can expose your entire subnetwork (i.e. configured for trunking wireless devices or controllers) to anyone connecting to the default network.

An attacker can also place a network-tapping device between the network and the wireless or wired device. These network-tapping products are readily available online and allow attackers to access network traffic, acting as a person-in-the-middle attack (PITMA). These devices can also be used to inject malicious code or websites into the in-transit traffic or provide attackers remote access with a reverse VPN tunnel.

Wireless infrastructure security must aim to prevent both physical access to wireless components (e.g. IoT lightbulbs that connect to Wi-Fi), as well as components that bridge back into the wired network.

2.3.9 WIRELESS INTRUSION DETECTION SYSTEMS (WIDS)

WIDS and wireless intrusion prevention systems (WIPS) are designed to detect and possibly mitigate active attacks that are carried out with radio frequency (RF) in the air. In combination with tools and protections on the wired network, air monitoring tools can help secure your wireless infrastructure by monitoring RF. Rogue APs are one such use case where WIDS and WIPS can help by locating and deactivating unauthorized access points that are connected into the wired network. Rogue APs are those that are not authorized and provisioned by the organization but are connected into the organization's network. These rogue APs can cause issues with security, by allowing poor encryption and authentication techniques (or none) and reduce visibility to the organization on what devices are connected, and where.

Having a WIDS or WIPS system can help reduce the time rogue AP devices are online, as otherwise they could go unnoticed indefinitely. Some WIDS or WIPS systems are integrated into the APs and use their radios for dual purposes, serving clients by listening to RF traffic and at other times acting as sensors in monitoring mode. Often these dual use applications reduce available time or bandwidth for users on an AP, due the fact the radio can only be in one mode (monitor mode) or the other (send and receive access point).

2.4 TRAINING BASED

Training needs to be mandated for both new and existing employees to ensure new threats and policy changes are properly communicated to users. Anyone that uses your wireless networks should have a good understanding on how to identify spoofed wireless networks, understand the difference between various Wi-Fi networks your company has provisioned and why this was done, what types of use are permitted on each SSID and VLAN segment, and how to properly connect to each needed wireless network. Users should also be aware of any processes on how and who to report wireless security incidents to and how they can get support.

2.4.1 GENERAL IT TRAINING

General IT training is a great foundation for security of wireless devices. You not only enhance work in cyber security, but also offer awareness on personal cyber security with wireless device usage. Important topics that should be covered include the systems available, the classes of data handled, the lifecycle of data, and the permissions assigned to the end user and the policies surrounding the use of Wi-Fi and network resources.

Users should have access to playbooks and procedures on the proper ways to interact with systems and data while maintaining security. These procedures should be reviewed regularly and updated to reflect changes with structure and software revisions.

2.4.2 DEVICE USE

Training should be provided on wireless standards and device usage. Showing users how to secure their own devices can have a positive impact on the workplace culture and security. Hosting sessions to demonstrate setting changes with a hands-on approach will add variety and keep visual learners engaged.

2.4.3 WI-FI SECURITY COURSES

There are various security courses offered online that can help improve general Wi-Fi security knowledge. Focus on courses designed to help average users. This training should cover topics for best practices around unencrypted and public Wi-Fi networks, VPNs, and mobile devices. Training should also cover awareness on the signs of a compromised device and the steps to take to address the issue.

3 ADDITIONAL CONSIDERATIONS

3.1 LEGAL IMPLICATIONS

Consider the legal implications of your policies and requirements before implementing them. Please note that this is not legal advice. Please seek a lawyer to ensure that you are following all Canadian laws correctly.

Some legal implications may be involved when personal equipment (e.g. BYOD or home equipment) is used. When having a penetration tester test your network, be sure to set boundaries, keep the scope to specific areas, and ensure they are trustworthy by checking industry reputation and references.

3.2 INCREASED TECHNICAL SUPPORT

Implementing the technical controls presented in this document will require additional technical support. Users may encounter roadblocks that prevent them from performing their tasks in a way they may be used to. Additional steps or configuration to devices that do not have these controls may be needed when implementing additional security controls. While it is necessary to protect your data, it is important to ensure that you have the resources available to assist with technical support.

3.3 AVAILABILITY

Availability is an important consideration. Without authentication or network infrastructure available, users cannot access resources they need. Considerations should be made to provide high availability and disaster recovery to the critical infrastructure. Multiple access points can be deployed in nearby areas to provide staggered coverage in the event of an outage.

Wireless signals are subject to jamming attacks and availability cannot be guaranteed. A robust wired network infrastructure with the ability for critical devices to be plugged in, as well as segregation between the wired and wireless networks are important considerations. This setup can ensure that any attacks on the wireless networks can be isolated and disconnected from the wired network if needed.

4 SUMMARY

It is critical that you implement proper policies surrounding Wi-Fi networks, as well as technical controls that will enforce your policies and provide proper training for your staff.

The wireless landscape is growing everyday with more smart-enabled devices with built-in Wi-Fi. The threat landscape has never been larger. Securing your network and being aware of the threats involved will help ensure you have a protected business environment for the future.

5 SUPPORTING CONTENT

5.1 LIST OF ABBREVIATIONS

Term	Definition
AD	Active Directory
AES	Advanced Encryption Standard
AP	Access Point
BYOD	Bring Your Own Device
CCCS	Canadian Centre for Cyber Security
CCMP	Cipher Block Chaining Message Authentication Code Protocol
CRC32	Cyclic Redundancy Check
CSE	Communications Security Establishment
DDoS	Distributed Denial of Service
EAP	Extensible Authentication Protocol
GC	Government of Canada
HIPAA	Health Insurance Portability and Accountability Act
IIROC	Investment Industry Regulatory Organization of Canada
IoT	Internet of Things
IT	Information Technology
ITS	Information Technology Security
LEAP	Lightweight Extensible Authentication Protocol
MFDA	Mutual Fund Dealers Association
OS	Operating System
PCI DSS	Payment Card Industry Data Security Standard
PEAP	Protected Extensible Authentication Protocol
PEAP-MS-CHAP	PEAP Microsoft Challenge Handshake Authentication Protocol
PI	Personal Information
PITMA	Person-In-The-Middle-Attack
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
RC4	Rivest Cipher 4
RF	Radio Frequency
SMB	Small Medium Business
SOHO	Small Office Home Office
SSID	Service Set Identifier
SSO	Single-Sign On

Term	Definition
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

5.2 GLOSSARY

Term	Definition
Authentication	A process or measure used to identify a user's identity
Bring Your Own Device (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.
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).
Confidentiality	The ability to protect sensitive information from being accessed by unauthorized people.
Distributed Denial of Service (DDoS) Attack	An attack in which multiple compromised systems are used to attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users
Encryption	Converting information from one form to another to hide its content and prevent unauthorized access.
Integrity	The ability to protect information from being modified or deleted unintentionally when it's not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
Internet of Things (IoT)	The network of everyday web-enabled devices that are capable of connecting and exchanging information between each other.
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.
Personal Information (PI)	Personal information is defined as information about an identifiable individual that is recorded in any form.
Threat	Any potential event or act (deliberate or accidental) or natural hazard that could compromise IT assets and information.
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.
Wi-Fi	Wi-Fi is a wireless technology that connects devices, like laptops and smart phones, to the Internet. It uses radio waves and a wireless router instead of a physical wired connection.

5.3 REFERENCES

Number	Reference
1	Canadian Centre for Cyber Security. ITSP.40.062 Guidance on Securely Configuring Network Protocols. October 2020.
2	Canadian Centre for Cyber Security. ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information. August 2016
3	Cnet. WeWork's weak Wi-Fi security leaves sensitive documents exposed. September 2019.
4	IoT World Today. IoT Cyberattacks Escalate in 2021, According to Kaspersky. September 2021.
5	Threat Post. Thousands of university Wi-Fi networks expose log-in credentials. September 2021.
6	Canadian Centre for Cyber Security. ITSG-33 IT Security Risk Management: A Lifecycle Approach. November 2018.
7	Canadian Centre for Cyber Security. ITSG-38 Network Security Zoning - Design Considerations for Placement of Services within Zones. May 2009.
8	Canadian Centre for Cyber Security. ITSAP.30.032 Best Practices for Passphrases and Passwords. September 2019.
9	Canadian Centre for Cyber Security. ITSP.70.012 Guidance for Hardening Microsoft Windows 10 Enterprise. March 2019.
10	Canadian Centre for Cyber Security. ITSAP.00.001 Using Your Mobile Device Securely. December 2020.