**Capstone Project**

**Printer & Document Solutions**

**Cybersecurity Guidelines**



Prepared for: Bazlur Rashid & Brett Turner

Prepared by: Daniel Gardiner

Student ID: 10537941

Submitted: 5th June 2022

# Additional Accessibility Instructions

## Enable Immersive reader Tool

In order to enable the text to speech function for this document/guide and other accessibility options such as increased spacing between words and lines, please refer to the following instructions (Microsoft, n.d.):

1. Select view in the options above
2. Select the *Immersive Reader* icon
3. With the *Immersive Reader* options now available, select which accessibility options you wish to adopt whilst reading this document/guide.

# Additional Notes on Accessibility

In addition to the above accessibility options within his document, the following accessibility guidelines have been adopted from the World Wide Web Consortium (W3C, 2018) in order to assist those requiring additional accessibility options, being:

***THE FOLLOWING ARE DRAFT ACCESSIBILITY IMPLEMENTATIONS.***

***FEEDBACK WILL BE REQUIRED BEFORE FINAL APPROVAL IS GIVEN.***

1. *Success Criterion 1.1.1: Non-text Content: Decoration, Formatting, Invisible*
2. *Success Criterion 1.4.1: Use of Colour*
3. *Success Criterion 1.4.3: Contrast Minimum*
4. *Success Criterion 1.4.4: Resize Text*

Whilst not all of the recommendations have or could be utilised within this document initially, any suggestions can be passed on to the document/guide’s authors for consideration.

# Document Control

## Document Information

|  |  |
| --- | --- |
|  | **Information** |
| Document Id | Printer & Document Solutions  Systems Guidelines/Playbook |
| Document Owner | Daniel Gardiner |
| Issue Date | 05/06/2022 |
| Last Saved Date | 05/06/2022 |
| File Name | CYB6014 - Deliverable Draft - Version Controlled |

## Document History

|  |  |  |
| --- | --- | --- |
| **Version** | **Issue Date** | **Changes** |
| 1.0 | 23/05/2022 | Prototype transitioned to draft deliverable |
| 1.01 | 27/05/2022 | Material in section 7 are completed |
| 1.02 | 29/05/2022 | Glossary completed |
| 1.03 | 30/05/2022 | Initial revision of document completed by COI |
| 1.04 | 31/06/2022 | Presentation of document to COI and further editing |
| 1.1 | 04/06/2022 | Deliverable completed. |

Please Note:

This document has been derived and modified from the publicly available instructions and template made available by the Government of Canada’s Public Services and Procurement Ministry (Public Services and Procurement Canada, 2021).

Contents

Additional Accessibility Instructions II

Enable Immersive reader Tool II

Additional Notes on Accessibility II

Document Control III

Document Information III

Document History III

1 Who is this guide for? IV

2 What this guide does NOT cover. V

3 Pre-Installation VI

3.1 Vendor/Manufacturer Requests VI

3.2 Requests to Vendors VI

3.3 Limiting Vendor Access VI

3.4 Physical Security VI

4 Ongoing Use VII

4.1 Device Location Security VII

4.2 Drivers & Associated Software Patches VII

4.3 Faults/Maintenance/Repairs VII

4.4 Device Configuration VII

5 Vendor Maintenance and Repairs VIII

5.1 Contacting the Vendor/Technical/Manufacturer VIII

5.2 Organising a Service Call VIII

5.3 Confirming vendor/repair agent identity VIII

5.4 Restricting Access VIII

5.5 Confirming Work Completed VIII

6 Destruction/Removal/Returning of Devices X

6.1 Responsible Handling of Data X

6.2 Prior to Device Removal/Destruction X

6.3 Device Destruction X

6.4 Returning the Device X

7 Access Controls XI

7.1 Authentication XI

7.2 Authorisation XI

7.3 Access XI

7.4 Manage XII

7.5 Audit XIII

List of references XIV

8 Glossary XVI

# Who is this guide for?

***Small to Medium Enterprises and Organisations***

Running a business or any small to medium organisation is difficult enough without having to worry about potential malicious actors attacking the livelihoods of you, your staff and even your customers via cyberattacks against your network.

Buying a printer, multi-function device or even a 3D printer sadly carries its own set of sometimes overlooked cybersecurity risks, to which this guide is designed to help mitigate against and assist your organisation in balancing both the convenience and risk associated with cybersecurity mitigation.

***Vendors***

Protecting your brand, suppliers, and your customers, is not only critical when it comes to minimising the financial risk that a successful cybersecurity attack could have on your organisation, but also reduces the chances that reputational damage can result from a successful and disclosed cyberattack against your customers that in some cases can be worse than the initial financial damage caused (Durbin, 2014).

Being open to the cybersecurity needs and wants of your customers will not only develop stronger customer relationships, but also solidify your organisation as being serious when combatting cybersecurity outside your own organisation.

***Individuals***

Regardless of one’s individual position or role within any business or organisation, protecting ourselves and our communities from the perils that malicious actors utilising cybersecurity threats present to us, is everyone’s responsibility and takes both enterprise wide and community wide diligence (NIST, 2018).

# What this guide does NOT cover.

1. Which brand or model you should purchase or use
2. Costs associated with purchasing, ongoing use or maintenance of the devices mentioned in this guide
3. Specific and individual security risks outside generic vendor software provided.
4. Specific cybersecurity response plans should you fall victim to cybercrime

# Pre-Installation

## Vendor/Manufacturer Requests

Prior to installation, vendors may make requests of you and potentially other key members of your organisation, which may or may not entail the following examples:

* Access to view the physical location to where the device/s are to be placed, to assess whether stairs need to be traversed and to confirm if there is adequate room for the devices to be installed
* Any particular configuration requests in both the driver/software included or hardware provided such as folding/stapling and binding attachments
* An understanding if you, the customer, have any particular requests of the vendor (See Below)

## Requests to Vendors

The key to creating a balance between an organisation’s cybersecurity policies and convenience for yourself and any other members of your organisation, is to make sure that your organisation places priority in terms of its policies over those that visitors, customers and guests would have when entering and potentially acting against such policies.

In the same way that vendors may have pre-installation requests as listed above, you and members of your organisation should very well look to make requests of vendors as long as they can be explained to avoid conflict and are fair and reasonable.

## Limiting Vendor Access

Limiting the access that vendors have to certain areas of your organisation are critical to avoiding physical security breaches and potentially even theft of property.

## Physical Security

As cybersecurity often refers to digital threats online, physical security is sadly overlooked and the growing number of vulnerabilities that printers and multifunction devices present are no exception to potential physical threats.

Wherever you decide to have your devices located is of course completely up to you, but when balancing security and convenience, remember that physical security can assist in protecting your data, network systems and even people (Hutter, 2016).

# Ongoing Use

## Device Location Security

In relation to the ongoing use of any printing, multifunction or 3D printer devices in any location, there are two main areas that can be looked at specifically to add extra security and reduce the risk that those outside your organisation may use to cause harm to you and your organisation (ACSC, 2022), being:

1. Preventing physical access to devices
2. Preventing observation of devices

Preventing *physical access* to devices from those that are not members of your organisation is critical to reducing access to exposed USB and network ports that could potentially be used to compromise the network from which said device is connected to.

Preventing and or reducing *observation* of devices prevents malicious actors from knowing what devices could potentially be targets they could target in a cyberattack.

## Drivers & Associated Software Patches

It is critical that all updates associated with your printing device are completed once they are made available. Although some vendors will provide the latest software updates that will allow for your printing device to work immediately, updates will occur over time as the manufacturer is made aware of issues with their original software and can also provide other new benefits to older, even outdated printing devices

(Symanovich, 2021).

The recommended timeframe for applying patches can vary, however devices such as printers, the *Essential Eight Maturity Model* (2021) recommends a timeframe

for updates on applications like those associated with printers, at within ***one month*** of the patch or software updates release.

## Faults/Maintenance/Repairs

Depending on if your printing device is subject to a warranty claim or is eligible for a service call out as part of the original sale or lease agreement, a fault or maintenance call also

# Vendor Maintenance and Repairs

## Contacting the Vendor/Technical/Manufacturer

It is important that contact details are correct and up to date should a warranty or service call be required to both troubleshoot issues either by offsite or onsite technical support. Having these details on hand and as accurate as possible will potentially reduce the devices downtime.

For warranty claims and technical support made over the phone, always contact the service provider on the details they have provided wherever possible and centralise these calls to be handled by those with access to such warranty, lease, and maintenance contracts available on hand.

## Organising a Service Call

Service calls should only be placed by both secure and pre-determined methods. For example, staff owned mobile phones or other IoT devices should be strictly avoided when making service calls or communicating with vendors and manufacturers at any time.

## Confirming vendor/repair agent identity

Should an apparent call be made from someone claiming to be a vendor, staff who would answer or respond to these calls should immediately filter them through to designated contacts (this may just be yourself if you are a small business owner and the business’s only employee) as this will assist with verification etc and avoid imitation or *spoofing* attacks by malicious actors.

## Restricting Access

There is a need to balance the needs of vendors to access your premises and your network whilst also protecting your printer and other critical network devices, but ultimately it is recommended to work with vendors whilst also helping them understand your needs and wants to protect your infrastructure from potential cybercriminals (Smith, n.d.).

Securing printing and associated network devices is covered in greater detail under the ***Access Controls*** section (See below).

## Confirming Work Completed

Once a vendor claims that the work required has been completed, depending if the work was successful or unsuccessful will decide the next steps that should be taken:

**If work is completed successfully:**

The authorised representative should be able to demonstrate that the work required has been completed and provide an overview of the maintenance/repair, installation, or removal of equipment to the business representative monitoring and waiting for the vendor or representative to complete their work.

There should be detailed documentation provided by the vendor for accurate record keeping should there be any associated issues with the work completed later on.

**If work is completed unsuccessfully:**

Should the authorised representative advise that work required has not or cannot be completed at this time, the authorised representative should communicate to the business owner or authorised person to discuss the next steps and supply detailed documentation advising of such steps.

# Destruction/Removal/Returning of Devices

## Responsible Handling of Data

One of the most overlooked areas of data security within an organisation is the hard drives and associated data storage devices that come with printers, especially those multi-function devices that have scanners and address books.

Any and all printer devices that are to be replaced or disposed of can produce risk and vulnerabilities if not handled properly. Like many other devices on the network in which data and information flows can be found, printers can have an internal hard drive that can potentially contain sensitive information, such as customer data and even intellectual property such as those found with 3D printers.

***Insert information surrounding unencrypted information stored of printer hard drives. Look into potential IP (instructions) stored in 3D printer hard drives.***

## Prior to Device Removal/Destruction

Any printing device that should fall under the category of being unable to be repaired, salvaged, or is not required to be retuned as part of any lease agreement, should be properly destroyed upon removing any identifying markers such as stickers, as well as any internal components that could be beneficial to malicious actors should they acquire them from e-waste depositories or by ‘dumpster diving’.

## Device Destruction

If a device is to be disposed of and has had all identifying markings and potential data storage hardware removed, the device/s can be flagged for destruction and can be transferred to the nearest available e-waste station in your local area.

## Returning the Device

Should a printing device be under lease or loan and must be returned when the agreement for such device/s is concluded, either by reaching the term date or from having to return/swap a device under warranty, a discussion with the vendor/manufacturer regarding the removal (or at the very least, erasure) of the internal hard drive should be conducted.

# Access Controls

At the very basic level, access control simply involves restricting access to the printer devices across your network where individual users, including employees, vendors and even guests would potentially have access to (Tunggal, 2021).

The National Institute of Standards and Technology (NIST) insists than an organisation develop policies, models as well as mechanisms when planning an access control system (Hu et al., 2006). However, the work involved in creating this for your individual business or organisation may not potentially be viable should you only have 1-2 staff and a smaller printer network than much larger organisations.

The following insights surrounding the key components that make up access control policy, provide further understanding of both how to identify and address potential security issues with your printers and associated network.

## Authentication

It is important to not only confirm the identity of somebody who may be using your printing devices and the networks they are connected to, but it is just as critical to establish a consistent and secure manner in which to do so.

Comparing any credentials, such as passwords and pin numbers, provided by any individual seeking to access a printing device (either physically or via the network), against the credentials stored authentication options are readily available, cost effective and sometimes included with your printing device/s (Identity Management Institute, n.d.).

Furthermore, 2FA & MFA (Two-Factor/Multi-Factor Authentication) protocols such as a text message confirmation or fingerprint scan are now almost a minimum standard for an organisation’s expected authentication requirements (Cloudflare, n.d.).

## Authorisation

Minimising the risk of unauthorised access to important information can be achieved with sound authorisation policies as part of an organisation’s access control policies (Australian Cyber Security Centre, 2020). The level of access that one has once authenticated can vary within an organisation, however as a benchmark to work from, no organisation’s printer network should be completely accessible by each and every individual within the organisation, as is highlighted by the policies of Zero Trust Security and Principle of Least Privilege(See *Manage* Below).

## Access

There are multiple forms of access control and methods for implementing them, with the most common outlined below, however it is important to note that whilst not every organisation will find these access controls suitable, it does provide a point into which an organisation’s needs and wants for access control can be developed.

***Mandatory Access Control (MAC):***

A form of access control that not only restricts what each individual authorised user has access to (both physical and network access) but also matches those restrictions to the specific printers or data held within those printers (Cloudflare, n.d.).

An example of this form of access control would be that only a certain individual has access to print, scan, or fax from 1 particular printing device.

***Role-based access control (RBAC):***

*Role-based access control* is focused on controlling what a group of individuals are authorised to be printing (following authentication which should also be checked each session) based on their role within the organisation.

For example, this form of access control would be suitable to only allow staff who need to print invoices in dispatch to have access to printing facilities on a printer based on their authorisation and prevent access to document retrieval and printing from certain parts of the organisation’s database.

***Discretionary Access Control (DAC):***

A system administrator can delegate permission for authorised users to access particular *parts* or objects on an organisations printer network and in turn that particular user can grant those identical permissions to other users.

*Warning: This approach to access control can increase the risk of cyberattack and other vulnerabilities as if the authorised user’s account/s were ever compromised, this would allow an attacker to delegate permissions to newly created malicious accounts they have added to the printer and other connected networks.*

## Manage

Regardless of the access control method used, management of the printers and their associated networks require constant revision and updating as the organisations grows and /or changes with it’s needs and wants to adjust.

Critically, when managing your printer devices, it is important to develop policies surrounding two key areas of cybersecurity access management, being *zero-trust security* and *principle of least privilege*.

***Please note: This approach to access control policy may not be suitable for a small to medium size enterprise as it takes an organisation-wide approach to meeting the goals of these access control management policies including both staff and equipment.***

***Zero-Trust Security:***

Essentially, as the name implies, *zero-trust security* establishes a policy that no individual, file, or printing device should be trusted completely on any given network and even when a level of trust is established, risk assessments are conducted continuously to accommodate for changes (Nguyen-Duy, 2022).

***Principle of Least Privilege:***

A key component of the *zero-trust security* model, the *principle of least privilege* forbids complete access to the entire printer network and allows for only the absolute bare minimum allocation of resources are allowed to be accessed by those authenticated users as part of their pre-determined authorisation privileges. Furthermore, the number of requests to and the time allocated to access any such printer or resource should be strictly time limited (CISA, 2013).

By providing members of an organisation with the bare minimum permission to access the printers and associated network, the risk of a malicious cybersecurity incident by outside actors or even an accidental incident occurring within the organisation are reduced (Australian Cyber Security Centre, 2020).

## Audit

It is important to implement and audit some form of monitoring system for the printer network within an organisation so as to accommodate the following critical points and reduce the risk of malicious activity across the network (Giese, 2022):

* What has been accessed?
* When was it accessed?
* Whom accessed it?
* Was anything else accessed in the same incident or shortly before/after?

Auditing is not just important for identifying cybersecurity vulnerabilities or potential attacks that have occurred or are even underway, but also allows for greater levels of compliance when dealing with internal and external departments that the affected organisation may have to report to and is best achieved by compiling all compliance policies surrounding printing devices and networks in general to a centralised policy document (Goldstein, N.d.).

# List of references

Australian Cyber Security Centre (ACSC). (2020, June 23). *Access Controls*. <https://www.cyber.gov.au/acsc/view-all-content/guidance/access-control>.

Australian Cyber Security Centre (ACSC). (2022, March 10). *Guidelines for Physical Security*. <https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-physical-security>.

Australian Cyber Security Centre (ACSC). (2021, October 6). *Accessing Security Vulnerabilities and Applying Patches*. <https://www.cyber.gov.au/acsc/view-all-content/publications/assessing-security-vulnerabilities-and-applying-patches>.

Cloudflare. (n.d.). What is Access Control? Authorisation vs Authentication. *Cloudlfare*. <https://www.cloudflare.com/en-gb/learning/access-management/what-is-access-control/>.

Cybersecurity & Infrastructure Security Agency (CISA). (2013, May 10). *Least Privilege*. <https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege>.

Durbin, S. (2014, May 30). Cybersecurity: The increasing threat to brand reputation. *Security Info Watch.* <https://www.securityinfowatch.com/cybersecurity/information-security/article/11489898/cyber-risk-increases-threat-to-brands>.

Giese, S. (2022, March 18). How to audit access controls across environments. *ITP.net*. <https://www.itp.net/security/how-to-audit-access-controls-across-environments>.

Goldstein, P. (n.d.). What is a Cybersecurity Audit and Why is it Important? *FedTech*. <https://fedtechmagazine.com/article/2021/06/what-cybersecurity-audit-and-why-it-important-perfcon>.

Hu, V., Ferraiolo, D, & Kuhn, D. (2006). *Assessment of Access Controls*. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7316.pdf>.

Hutter, D. (2021). *Physical Security and Why It Is Important*. [White paper]. SANS

Institute. <https://sansorg.egnyte.com/dl/MEttXe0pg2>.

Identity Management Institute. (n.d.). Access Control Types and Models. *Identity Management Institute*. <https://identitymanagementinstitute.org/access-control-types-and-models/>.

Microsoft. (n.d.). *Make your Word documents accessible to people with disabilities*. <https://support.microsoft.com/en-us/office/make-your-word-documents-accessible-to-people-with-disabilities-d9bf3683-87ac-47ea-b91a-78dcacb3c66d#bkmk_whileyouwork_win>.

National Institute of Standards and Technology. (2018). *Cybersecurity is Everyone’s Job*. <https://www.nist.gov/system/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf>.

Nguyen-Duy, J. (2022, January 28). Least Privilege Access and Zero Trust. *Fortinet*. <https://www.fortinet.com/blog/ciso-collective/least-privilege-access-and-zero-trust>.

Project Service and Procurement Canada. (2021). *Project Charter Introduction*. <https://www.tpsgc-pwgsc.gc.ca/biens-property/sngp-npms/ti-it/etivcapft-idsfvpcvc-eng.html>.

Smith, C. (n.d.). Limit Privileged Access for Third-Party Vendors Without Restricting their Ability to get Work Done. *Delinea*. <https://delinea.com/blog/limit-access-for-third-party-vendors>.

Symanovich, S. (2021, January 23). 5 Reasons why general software updates and patches are important. *NortonLifeLock*. <https://us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html>.

Tunggal, Abi Tyas. (2021, January 14). What is Access Control? The Essential Cybersecurity Practice. *UpGuard*. <https://www.upguard.com/blog/access-control>.

WC3. (n.d.). *Web Content Accessibility Guidelines (WCAG) 2.1*. <https://www.w3.org/TR/2018/REC-WCAG21-20180605/#perceivable>.

# Glossary

**Access Controls.** A set of cybersecurity policies that dictate, who is allowed to access data or devices and the manner in which they can access them i.e. Authorised to access only certain printers and only certain features of such printer.

**Authentication.** The process of verifying the credibility of an individual, group of individuals, computer software or devices/s that seek to perform certain acts or access certain devices, physical spaces, or data.

**Authorisation.** The process of providing the ability of an individual, group of individuals, computer software or device/s to make certain, usually predetermined actions it otherwise could not do without.

**Accessibility.** The level or way in which something is accessible to others, in particular the way in which those with disabilities are able to access, read and interact with documents such as this.

**Cyberattack.** An attack, typically against a device on a network (including the internet), that can be for the purposes of theft or spying.

**Cybersecurity.** A measure or set of measures designed to prevent cyberattacks.

**Data.** A collection of factual numbers,words, statistics etc. that are used for generating accurate calculations, assertions and/or outcomes.

**Printer Driver.** Software that allows for the communication between an operating system (Windows/Mac/Linux etc.)and a printer, multifunction, or 3D printing device.

**Essential Eight.** A set of guidelines that mitigate the risks of a cyber criminals successfully completing a cyberattack.

**Firmware.** A hybrid of both software and hardware that is usually permanently embedded in computer hardware, including printing devices.

**Printer.** A device that can transplant text and images onto various paper stocks using either inkjet or laser-based technologies.

**Multifactor Authentication.** A process in which an individual or group of individuals are verified (authenticated) before becoming authorised users on a device such as a printer or a network.

**Multifunction Printer (MFP).** In addition to being a printer, a multifunction device or MFP, also provides features such as a digital fax machine, scanner, or stapling device.

**National Institute of Standards and technology (NIST).** A non-regulatory organisation based in the United States that, amongst other endeavours, seeks to promote and enhance better standards of cybersecurity and publishes documents and guides in order to do so.

**Software.** Pre-programmed procedures in the form of computer code that control the functions of both hardware and other software applications.

**Vendor.** An individual, business or organisation that seeks to sell or provide a product or service to others either for monetary cost or return of service.