**Capstone Project**

**Printer & Document Solutions**

**Cybersecurity Guidelines**



Prepared for: Bazlur Rashid & Brett Turner

Prepared by: Daniel Gardiner ID 10537941

Submitted: 10th April 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 author’s for consideration.

# Document Control

## Document Information

|  |  |
| --- | --- |
|  | **Information** |
| Document Id | Printer & Document Solutions  Systems Guidelines/Playbook |
| Document Owner | Daniel Gardiner |
| Issue Date | 03/02/2022 |
| Last Saved Date | 09/04/2022 |
| File Name | Capstone Project – Version Controlled Document |

## Document History

|  |  |  |
| --- | --- | --- |
| **Version** | **Issue Date** | **Changes** |
| 1.00 | 24/02/2022 | Initial document creation |
| 1.02 | 25/03/2022 | Draft headings created and 1st QA test completed |
| 1.06 | 31/03/2022 | Accessibility guidelines and options are created |
| 1.07 | 01/04/2022 | 3rd QA test completed |
| 1.10 | 09/04/2022 | Draft prototype ready for stakeholder feedback |

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 IX

6.1 Responsible Handling of Data IX

6.2 Prior to Device Removal/Destruction IX

6.3 Device Destruction IX

6.4 Returning the Device IX

7 TBA X

7.1 TBA X

7.2 TBA X

List of references XI

8 Glossary XII

# 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 as the manufacturer is made aware of issues with their original software

## 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

## Device Configuration

***THIS HEADING REQUIRES FEEDBACK BEFORE IMPLEMENTATION***

# 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.

For warranty claims and technical support made over the phone, always contact the service provider on the details they have provided.

## Organising a Service Call

Service calls should only be placed by both secure and pre-determined methods. For example, individual staff mobile hone or other IoT devices should be avoided when making service call,

## 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

## Restricting Access

***PENDING FURTHER RESEARCH***

## Confirming Work Completed

***THIS HEADING REQUIRES FEEDBACK BEFORE IMPLEMENTATION***

# 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

# TBA

## TBA

## TBA

# List of references

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

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>.

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

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

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>.

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>.

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

# Glossary