CyFun®

SMALL

CyberFundamentals 2023

Version 2023-03-01

TABLE OF CONTENTS

INTRODUCTION

The **CyberFundamentals Framework** is a set of concrete measures to:

- protect data,
- significantly reduce the risk of the most common cyberattacks,
- increase an organisation's cyber resilience.

To respond to the severity of the threat that an organisation is exposed to, and in addition to the starting level **Small**, three assurance levels are also provided: **Basic, Important and Essential**.

The **starting level Small** allows an organisation to make an initial assessment, excluding the aspects relating to the internal development of applications.

The starting level Small is intended for micro-organisations (except those in high-risk environments) or organisations with limited technical knowledge.

The framework is a living document and will continue to be updated and improved, taking into account the feedback received from stakeholders, the evolving risk of specific cybersecurity threats, the availability of technical solutions and the insights achieved over time.

1. PROTECT ALL LOGINS WITH MULTI-FACTOR AUTHENTICATION

- **Use Multi-Factor Authentication whenever possible.**
- **Always use Multi-Factor Authentication when accessing systems remotely**

Guidance

Most Multi-Factor Authentication tools combine your password with things that you have (a smartphone, a badge or an ID card) or things you are (a fingerprint). Using multiple elements to authenticate reduces the risk of hacking.

- Use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security.
  If you opt for a typical password:
  - Make it long, with lower- and upper-case characters, possibly also numbers and special characters.
  - Avoid obvious passwords, such as "password", sequences of letters or numbers like "abc", numbers like "123".
  - Avoid using personal info that can be found online.
- And whether you use passphrases or passwords
  - Do not reuse them elsewhere.
  - Change your password as soon as you suspect that they have been compromised.
- Enable Multi-Factor Authentication. There are a lot of MFA tools available, it is best to choose an MFA tool that offers a variety of authentication options.
  MFA is of the utmost importance for internet-facing systems such as for example remote access. Remote access can be achieved using systems such as VPN (Virtual Private Network) or RDP (Remote Desktop Protocol).

2. INSTALL ALL SECURITY UPDATES IMMEDIATELY

- **Implement security updates/patches for all your software as soon as they are available.**

Guidance

- As developers battle with cybercriminals and try to make their software more secure and less vulnerable to the latest attacks, patching as soon as possible is the key to increased cybersecurity.
- Consider the measures listed below:
  - Only install those applications (operating systems, firmware, or plugins) that you need to run your organisation.
  - Install only vendor-supported versions of software you want to use.
  - Automate the update process as much as possible by setting automatic updates as the default setting on your endpoints' operating systems.
  - There are products that can scan your system and notify you when there is an update for an application you have installed. If you use one of those products, make sure it checks for updates for every application you use. If you don't use those products, designate a day each month to check the availability of new patches and install them.

3. INSTALL ANTI-VIRUS

- **Implement an anti-virus solution on all types of devices and keep it up to date in order to ensure its continuous effectiveness.**

Guidance

Even with the best precautions, you can be faced with an intrusion by a virus or by malware. Anti-malware software is a secondary barrier that protects you from the impact of cyber-incidents.

- The anti-malware software that you select should protect against all kinds of malware such as viruses, spyware, adware and rootkits.
- It is recommended to set the anti-malware software to automatically check for updates at least daily (or when available in "real-time"), and then run a full scan soon afterwards. If multiple devices (home computers, laptops, tablets…) are used, anti-malware software should be installed and updated on all those devices.
- As a preventative measure, the following rules should be applied:
  - Do not share USB drives or external hard drives between personal and business computers or devices.
  - Do not connect any unknown or untrusted hardware into your system or network and do not insert any unknown external USB drive. These devices may have malware on them. Disable the AutoRun feature for portable drives (USB, Optical…) on your business computers to help prevent such malicious programs from installing themselves on your systems.
  - Do not install pirated software as it may contain malware.

4. SECURE YOUR NETWORK

- **Protect your network by installing a firewall.**
- **Protect data on the network accessed via Wi-Fi using wireless encryption standards.**
- **Pay specific attention to remote access security.**

Guidance

- Don't share you Wi-Fi passwords with anyone.
- If needed, separate your Guest/Visitors' Wi-Fi network from your professional network.
- Firewalls should be installed and configured between your internal network and the internet. This may be a function of a (wireless) access point/router, or it may be a function of a router provided by the Internet Service Provider (ISP). The firewalls should be activated and updated. You might check your ISP service catalogue on the Network security services provided.
  - Ensure that the administrative password of your firewall is changed upon installation and regularly thereafter. Also consider changing the administrator's log-in
  - Encryption makes your electronically stored information unreadable to anyone who does not have the correct password or key. Set your router to use at least Wi-Fi Protected Access (WPA-2 or WPA-3 where possible), with the Advanced Encryption Standard (AES) for encryption.

5. BACK UP YOUR DATA

- **Regularly perform automated backups of your information.**
- **Put a backup OFF LINE (not connected to the network) weekly or every few weeks.**
- **After major changes, back up your systems so you can restore them more easily.**

Guidance

Think about how much you rely on your organisation-critical data. Creating and testing backups will allow you to restore your data and ICT systems in the event of a major cybersecurity incident (e.g. a ransomware attack).

Here are some basic guidelines to consider:

- Identify what data you need to back up. This is the essential data/information that your organisation couldn't function without.
- Determine the back-up frequency based on the amount of data (updated or created) that will be lost or will need to be re-entered after an outage.
- Separate back-up media from your other storage systems. An offline backup is very important to limit the possibility that your back up also becomes encrypted or wiped if your system is hacked.
- Test restoring the data at regular intervals. This is also a basic check to find out whether the backup procedure is working fine.

6. ADMINISTRATION RIGHTS

- **Ensure that no-one works with administrator privileges for daily tasks.**

Guidance

An administrator has a lot of access to your system. Protecting these accounts is very important because they have a lot of value to cybercriminals. Consider the following principles to protect these accounts:

- Separate administrator accounts from user accounts. For everyday tasks, a user account without administrator privileges will suffice.
- Require Multifactor Authentication for all access via administrator accounts.

7. FINAL RECOMMENDATIONS

- **Physically protect your computers and mobile devices against theft or improper use.**
- **Restrict access to premises, backups, servers, and network components to authorised individuals only.**
- **Know who to contact and how in the event of a cyber incident.**

Guidance

- Physical security and access restriction:
  - Physical security involves the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to your organisation.
  - Affordably priced mobile device management systems are available. These can be an option if you use mobile devices a lot. Enabling applications such as "Find My Phone" on your mobile phones can be a first step.
  - Strictly manage keys to access the premises and alarm codes.
- If an incident occurs:
  - Keep an offline copy (e.g. offline hard disk or laptop, paper hardcopy, ...) of any document you are likely to need during a cybersecurity incident or crisis by answering the following questions:
    - Who do I need to contact in the event of a cyber incident?
    - What details do I need to contact them?
    - Which information will they ask for?
  - See also our recommendations in the CCB Cyber Security Incident Management guide, which provides a pragmatic approach towards handling cybersecurity incidents and can be used as inspiration for your own incident response plan or playbook.

Disclaimer

This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

All texts, layouts, designs and other elements of any nature in this document are subject to **copyright law**. The reproduction of extracts from this document is authorised for non-commercial purposes only and provided that the source is acknowledged.

This document contains technical information written mainly in English. This information relating to the security of networks and information systems is addressed to IT services which use the English terms of computer language. A translation into Dutch, French or German of this technical information is also made available the CCB.

The CCB accepts **no responsibility for the content** of this document.
The information provided:

- is exclusive of a general nature and is not intended to take into consideration all particular situations.
- is not necessarily exhaustive, precise, or up to date on all points.

Responsible editor

Centre for Cybersecurity Belgium
Mr. De Bruycker, Director-General
Rue de la Loi, 18
1000 Brussels

Legal depot
D/2023/14828/001

Centre for Cybersecurity Belgium

Rue de la Loi, 18

1000 Brussels