



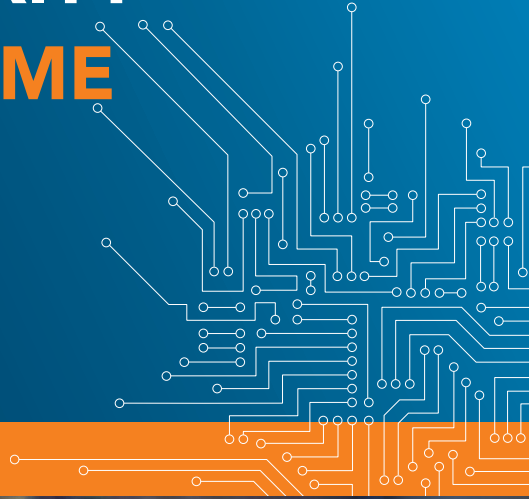
CENTRE FOR  
CYBER SECURITY  
BELGIUM



CYBER SECURITY  
COALITION.

# CYBER SECURITY GUIDE FOR SME

/ BELGIUM



.be

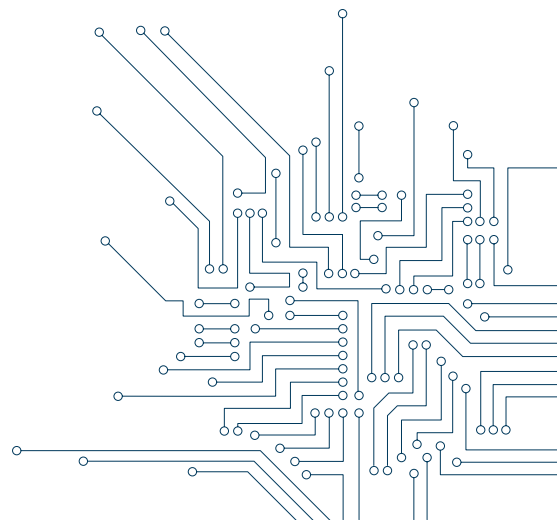
## ABOUT THIS GUIDE

---

THIS CYBER SECURITY GUIDE WAS DEVELOPED BY THE CENTRE FOR CYBER SECURITY BELGIUM (CCB) IN PARTNERSHIP WITH THE CYBER SECURITY COALITION BELGIUM FOR SMALL AND MEDIUM-SIZED ENTERPRISES (SME). IT IS BASED ON INPUT AND BEST PRACTICES FROM PRIVATE AND PUBLIC ENTITIES.

The goal is to provide SMEs with an overview of basic and more advanced cyber security measures. Where all SMEs should implement cyber security according to the result of their own risk assessments, this guide provides a quick list of security controls that might or should be implemented.

This guide should enable SMEs to improve their cyber security levels, reduce cyber security risks, mitigate vulnerabilities and improve their resilience. It will provide an easy framework so that small and medium-sized enterprises can safely integrate their businesses into a worldwide round-the-clock marketplace.



## THE CENTRE FOR CYBER SECURITY BELGIUM

---



THE CENTRE FOR CYBERSECURITY BELGIUM (CCB) IS THE CENTRAL AUTHORITY FOR CYBER SECURITY IN BELGIUM.

The CCB was created by Royal Decree of 10 October 2014. It is scheduled to draft a national Cyber Security policy and encourage all relevant Belgian government departments to make an adequate and integrated contribution. The CCB operates under the authority of the Prime Minister and relies on the administrative and logistical support of the Federal Public Service Chancellery of the Prime Minister to carry out its assignments. Please visit [www.ccb.belgium.be](http://www.ccb.belgium.be) for a complete overview of the Centre's tasks.

## THE CYBER SECURITY COALITION

---



THE CYBER SECURITY COALITION IS A UNIQUE PARTNERSHIP BETWEEN PLAYERS FROM THE ACADEMIC WORLD, THE PUBLIC AUTHORITIES AND THE PRIVATE SECTOR WHO ARE JOINING FORCES IN THE FIGHT AGAINST CYBERCRIME.

More than 50 key players from across these 3 sectors are currently active members contributing to the Coalition's mission and objectives. The Coalition answers the urgent need for a cross-sector collaboration to share knowledge and experience, to initiate, organise and coordinate concrete cross-sector initiatives, to raise awareness among citizens and organisations, to promote the development of expertise, and to issue recommendations for more efficient policies and regulations.

## FOREWORD

---

**SMALL AND MEDIUM SIZE ENTERPRISES (SMES) ARE AN IMPORTANT DRIVER FOR INNOVATION AND GROWTH IN BELGIUM.**

Cybercrime in the SME environment is a growing concern. Unlike large organizations, most SMEs do not have their own dedicated cyber security teams (CSIRTs). Cyber criminals seeking to gain financial advantage or cause damage to companies tend to look for easier targets. Furthermore, SMEs' dependency on Information Technologies and the Internet has opened the door to vulnerabilities to cybercrime. These weaknesses are making information security a critical issue for all SMEs.

Featuring cyber security measures for Small and Medium Enterprises, this guide was created by the Centre for Cyber security Belgium (CCB) in close collaboration with the Cyber Security Coalition. We have developed a list of 12 cyber security topics with basic and advanced cybersecurity recommendations SMEs can use to reduce exploitable weaknesses and vulnerabilities and defend against data breaches and cyber-attacks.

The basic recommendations in this guide help SMEs to get a head start in terms of security. They help to avoid the most common traps and to protect your most valuable data. The advanced best practices and tips help to adopt even better protection techniques.

**MIGUEL DE BRUYCKER**  
Managing Director Centre  
for Cyber security  
Belgium (CCB)

**CHRISTINE DARVILLE**  
Chairwoman of the  
Cyber Security Coalition

## CONTENTS

---





<b>01</b>	<b>INVOLVING TOP MANAGEMENT</b>	<b>06</b>
<b>02</b>	<b>PUBLISH A CORPORATE SECURITY POLICY AND A CODE OF CONDUCT</b>	<b>08</b>
<b>03</b>	<b>RAISE STAFF AWARENESS OF CYBER RISKS</b>	<b>10</b>
<b>04</b>	<b>MANAGE YOUR KEY ICT ASSETS</b>	<b>12</b>
<b>05</b>	<b>UPDATE ALL PROGRAMS</b>	<b>14</b>
<b>06</b>	<b>INSTALL ANTIVIRUS PROTECTION</b>	<b>16</b>
<b>07</b>	<b>BACKUP ALL INFORMATION</b>	<b>18</b>
<b>08</b>	<b>MANAGE ACCESS TO YOUR COMPUTERS AND NETWORKS</b>	<b>20</b>
<b>09</b>	<b>SECURE WORKSTATIONS AND MOBILE DEVICES</b>	<b>22</b>
<b>10</b>	<b>SECURE SERVERS AND NETWORK COMPONENTS</b>	<b>24</b>
<b>11</b>	<b>SECURE REMOTE ACCESS</b>	<b>26</b>
<b>12</b>	<b>HAVE A BUSINESS CONTINUITY AND AN INCIDENT HANDLING PLAN</b>	<b>28</b>

# 01

## INVOLVING TOP MANAGEMENT





### BASIC PROTECTION

---

-  **Appoint** an information security officer
-  **Identify** your ICT risks and safeguard your business for the future
-  **Strive** to comply with privacy, data handling and security legal and regulatory requirements
-  **Be aware** of cyber threats and vulnerabilities in your networks

### ADVANCED PROTECTION

---





-  **Make** sure the information security officer is operating independently and not part of ICT
-  **Clearly** define the objectives of the system and network monitoring
-  **Identify** the business and legal consequences of data leakage, network failure ...
-  **Periodically carry out** risk and security audits, with the results and the action plan being briefed at C-level











# 02

## PUBLISH A CORPORATE SECURITY POLICY AND A CODE OF CONDUCT

### BASIC PROTECTION

-  **Create** and apply procedures for the arrival and departure of users (personnel, interns, etc.)
-  **Describe** security roles and responsibilities (for physical, personnel & ICT security)
-  **Develop** and distribute a code of conduct for using ICT
-  **Plan** and execute security audits

### ADVANCED PROTECTION

-  **Create** a classification and marking scheme for sensitive information
-  **Introduce** concepts of need to know, least privilege and segregation of duties into your policies and business processes
-  **Publish** a Responsible Disclosure policy
-  **Have** sensitive documents stored in locked closets
-  **Have** sensitive documents destroyed using a shredder
-  **At** the end of the working day have any documents left on the printer **shredded**
-  **Enforce** the locked print option when available
-  **Develop** a cyber security training concept and plan





# 03

## RAISE STAFF AWARENESS OF CYBER RISKS

### BASIC PROTECTION

---

- 📄 **Get** users to subscribe to your code of conduct
- 📄 **Periodically remind** users of the importance of their secure behaviour
- 📄 **Periodically remind** users that information must be treated as sensitive & with respect for privacy rules
- 📄 **Inform** users how to recognize phishing (e-mail fraud) and how to respond
- 📄 **Inform** your employees of the occurrence of "CEO-Fraud", install sufficient control on the execution of payments

### ADVANCED PROTECTION

---

- 📄 **Make** knowledge of and respect for the code of conduct part of the personnel evaluation process
- 📄 **Periodically evaluate** users' awareness and responsiveness





# 04

## MANAGE YOUR KEY ICT ASSETS







### BASIC PROTECTION

---

-  **Maintain** an inventory of all ICT equipment and of software licenses
-  **Create** an accurate and up-to-date map of all your networks and interconnections

### ADVANCED PROTECTION

---

-  **Use** configuration management tools (or at the very least a tool such as Microsoft MMC ...)
-  **Define** a baseline security configuration
-  **Contracts** and SLAs (Service Level Agreements) include a security clause
-  **Implement** a change control process
-  **Implement** a uniform level of security across your networks
-  **Audit** all configurations regularly (including servers, firewalls and network components)






# 05

## UPDATE ALL PROGRAMS




### BASIC PROTECTION

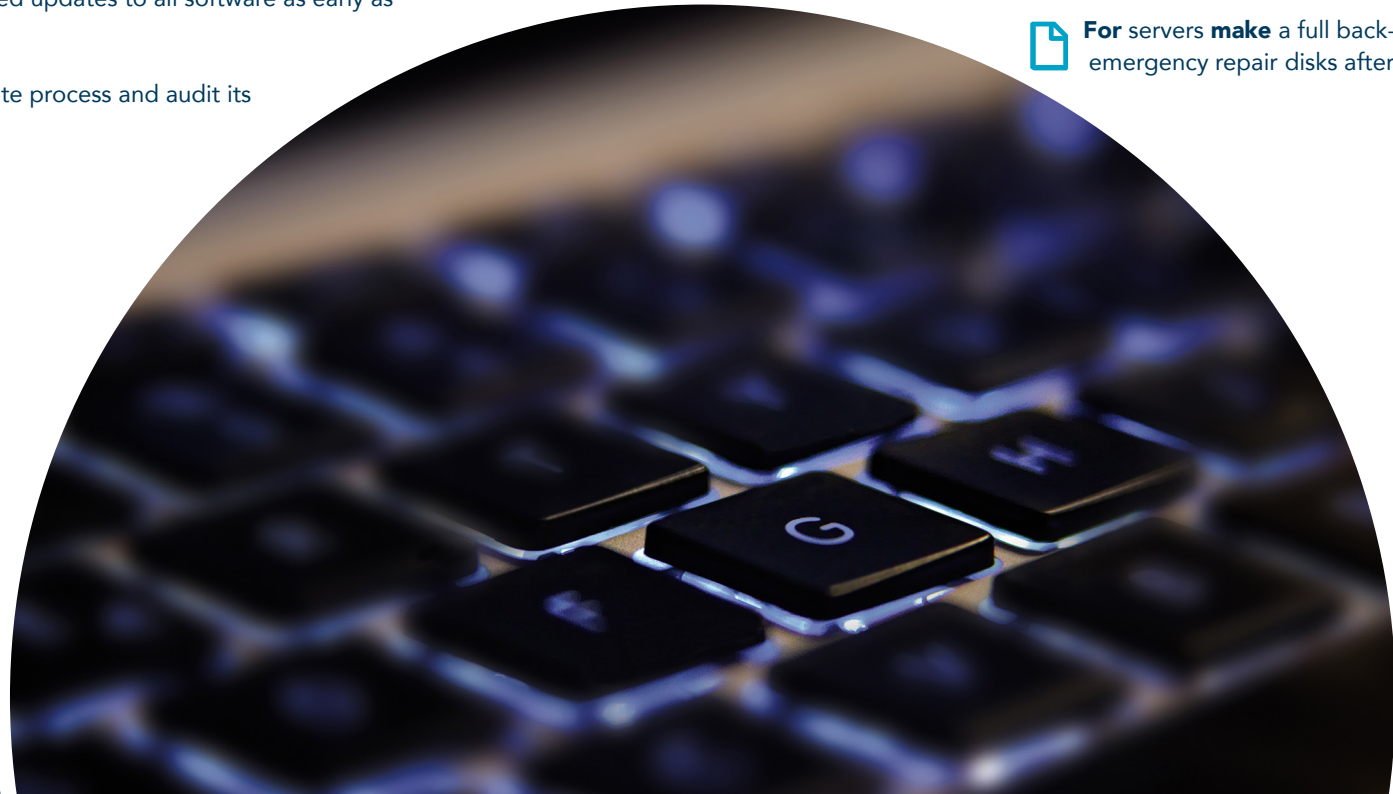
---

-  **Create** an in-house patch, patch and path culture (workstations, mobile devices, servers, network components ...)
-  **Apply** security related updates to all software as early as possible
-  **Automate** the update process and audit its efficiency

### ADVANCED PROTECTION

---

-  **Develop** a reference and test environment for new patches
-  **Update** all third-party software such as browsers and plugins
-  **For servers make** a full back-up before and create emergency repair disks after updating








# 06

## INSTALL ANTIVIRUS PROTECTION




### BASIC PROTECTION

---

-  **Antivirus** software is installed on all workstations and servers
-  **Automate** updates of antivirus products
-  **Users** are familiar with the antivirus software's infection warning procedure

### ADVANCED PROTECTION

---

-  **All virus warnings** are analyzed by an ICT expert
-  **Antivirus** software is installed on all mobile devices
-  **The antivirus software** is regularly tested with fingerprint solutions






# 07

## BACKUP ALL INFORMATION




### BASIC PROTECTION

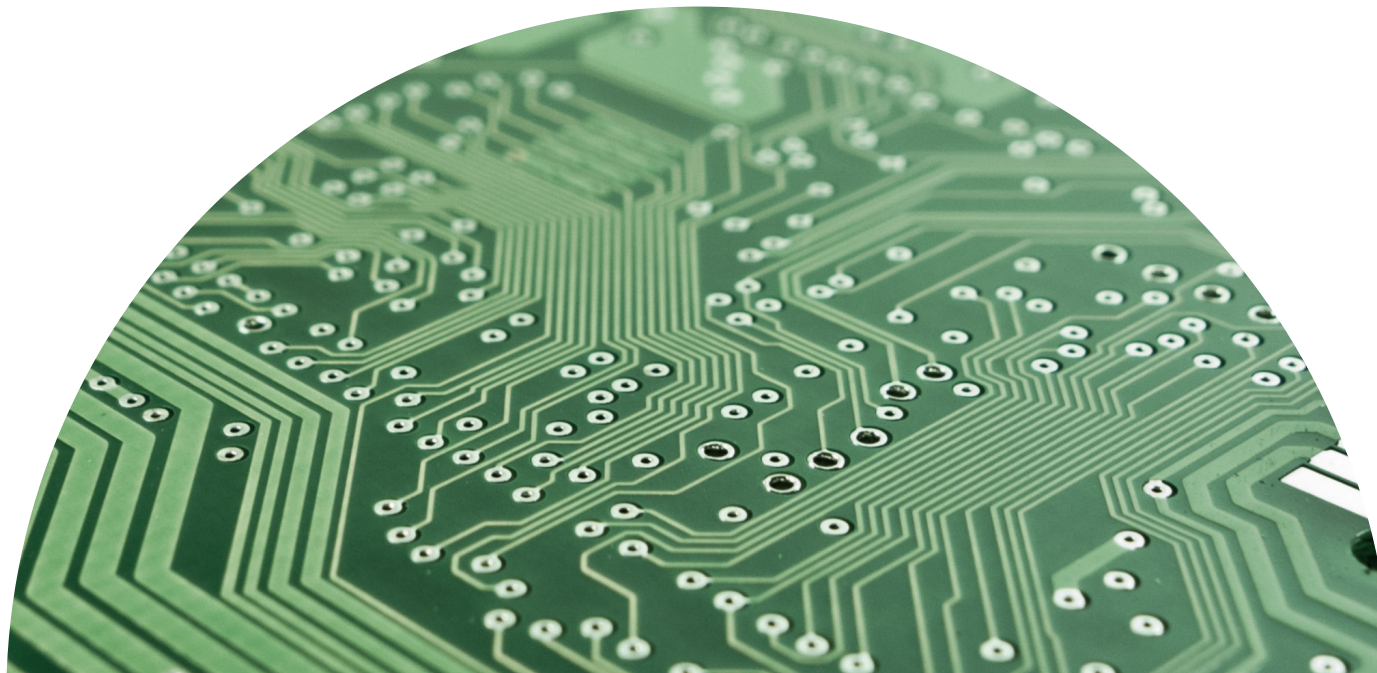
---

-  **Daily backups** of your important data
-  **Select** own or cloud backup solutions
-  **Store** Backups offline and in a separate place (at a distance from their source if possible)

### ADVANCED PROTECTION

---

-  **Backups** are stored in a safe or in a secure data centre
-  **Periodic** restoration tests are carried out in order to check the quality of the backups
-  **Encrypt** data stored in the cloud











# 08

## MANAGE ACCESS TO YOUR COMPUTERS AND NETWORKS










### BASIC PROTECTION

---

-  **Change** all default passwords
-  **No one** works with administrator privileges for daily tasks
-  **Keep** a limited and updated list of system administrator accounts
-  **Passwords** must be longer than 10 characters with a combination of character types and changed periodically or when there is any suspicion of compromise
-  **Use** only individual accounts and never share passwords
-  **Immediately disable** unused accounts
-  **Enforce** authentication and password rules
-  **Rights** and privileges are managed by user groups

### ADVANCED PROTECTION

---





-  **Users** are only authorized to access the information they need to perform their duties
-  **Search** and lock unused accounts
-  **Use** multi-factor authentication
-  **Block** access to the Internet from accounts with administrator rights
-  **Search** for abnormal access to information and systems (timeframes, applications, data ...)
-  **Frequently audit** the central directory (Active Directory or LDAP directory)
-  **Limit** employee access with a badge system and create multiple security zones
-  **Register** all visits
-  **Ensure** office cleaning is carried out during working hours or under permanent surveillance

# 09

## SECURE WORKSTATIONS AND MOBILE DEVICES



### BASIC PROTECTION

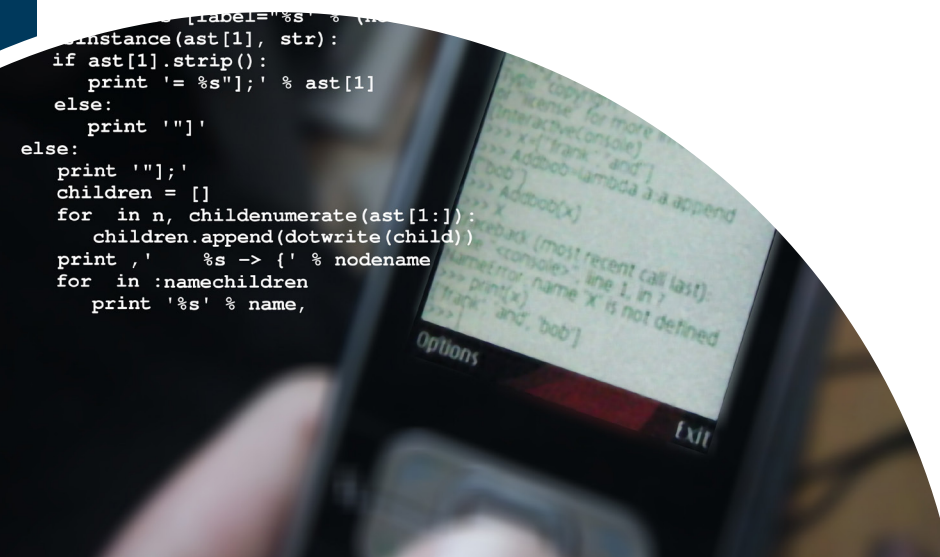
---

-  **Automatically lock** workstations and mobile devices when unused
-  **Laptops**, smartphones or tablets are never left **unattended**
-  **Disable** autorun functions from external media
-  **Store** or copy all data on a server or a NAS (Network Area Storage)

### ADVANCED PROTECTION

---

-  **Decommissioned** hard drives, media and printer storage are physically **destroyed**
-  **Prohibit** the connection of personal devices to the organization's information system
-  **Encrypt** laptop hard disks
-  **Sensitive** or confidential data must be encrypted for transmission
-  **Technical** measures are applied to prevent the connection of unregistered portable media
-  **The data** stored in the cloud is encrypted (e.g. BoxCryptor)
-  **The guarantees** offered by the cloud provider correspond to the stored information's level of criticality
-  **External media** such as USB drives are checked for viruses before they are connected to a computer












# 10

## SECURE SERVERS AND NETWORK COMPONENTS











### BASIC PROTECTION

---

-  **Change** all default passwords and disable unused accounts
-  **The wifi network** is protected by WPA2 encryption
-  **Shut down** unused services and ports
-  **Avoid** remote connections to servers
-  **Use** secure applications and protocols
-  **Security logs** on servers and firewalls are kept for a period of at least 1 month
-  **The guest wifi network** is separated from the corporate network

### ADVANCED PROTECTION

---




-  **Security logs** are kept for a period of at least 6 months
-  **The corporate wifi network** is protected by WPA2 Enterprise with device registration
-  **Harden** all systems according to vendor recommendations
-  **For** the administration of servers, **use a network** that is (logically) separated from the user network
-  **Evaluate** all server, firewall and network component events/alerts
-  **An analysis** and warning system **uses the logs** in order to detect any malicious behaviour (SIEM)
-  **An IDS/IPS** (Intrusion Detection/Prevention System) monitors all communications
-  **Physical access** to servers and network components limited to a minimum number of people
-  **Any physical access** to servers and network components is registered
-  **Perform** penetration tests and vulnerability scans

# 11

## SECURE REMOTE ACCESS




### BASIC PROTECTION

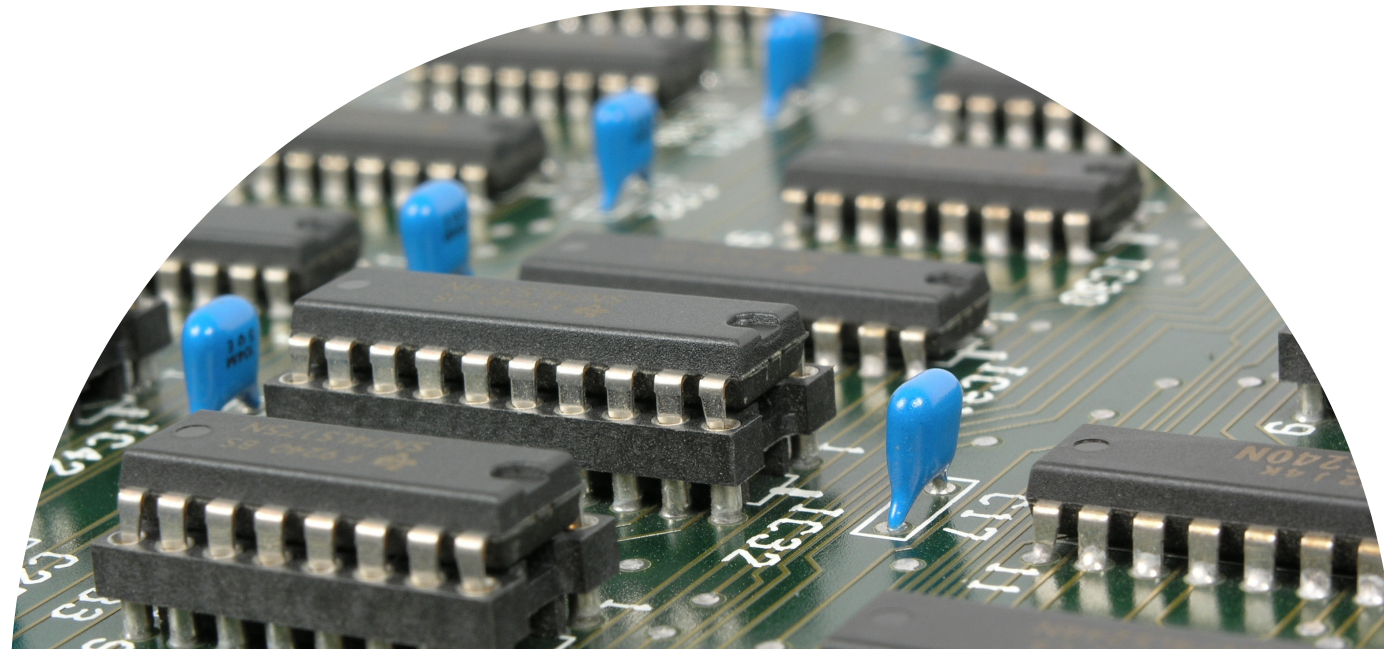
---

-  **Remote** access must be closed automatically when inactive for a certain amount of time
-  **Limit** remote access to what is strictly necessary
-  **All connections** to the corporate network are secured and encrypted

### ADVANCED PROTECTION

---

-  **Allow** only Virtual Private Network (VPN) connections for end points
-  **Strong authentication** is required when connecting from external public networks
-  **Remote** access is limited to the IP addresses of the providers and regions needed








# 12

## HAVE A BUSINESS CONTINUITY AND AN INCIDENT HANDLING PLAN




### BASIC PROTECTION

---

-  **Create** an Incident Handling Plan to respond to an incident
-  **Create** a Business Continuity Plan to preserve business
-  **All employees** must know the contact point for reporting incidents
-  **Distribute** and update contact point information (internal and external contacts, management and technical contacts ...)
-  **Report** all incidents to C-level

### ADVANCED PROTECTION

---

-  **Evaluate** and test these plans every year
-  **Evaluate** the opportunity for cyber security incident insurance coverage
-  **Install** fall-back capabilities for utilities (electricity, phone, internet, ...)



## DISCLAIMER

---

THIS GUIDE HAS BEEN PRODUCED BY THE CENTRE FOR CYBER SECURITY BELGIUM. ALL TEXTS, LAYOUTS, DESIGNS AND ELEMENTS OF ANY KIND IN THIS GUIDE ARE PROTECTED BY COPYRIGHT. EXTRACTS FROM THE TEXT OF THIS GUIDE MAY BE REPRODUCED FOR NON-COMMERCIAL PURPOSES ONLY, PROVIDED THAT THE SOURCE IS SPECIFIED. THE CENTRE FOR CYBER SECURITY BELGIUM DISCLAIMS ANY LIABILITY FOR THE CONTENT OF THIS GUIDE.

The information provided :

- Is exclusively of a general nature and not geared towards the specific situation of any individual or legal entity
- Is not necessarily complete, accurate or up to date
- Does not constitute professional or legal advice
- Does not replace expert advice
- Does not provide any warranty for secure protection.

## SPONSORS

---



**BNP PARIBAS**  
**FORTIS**



**Deloitte.**



**proximus**



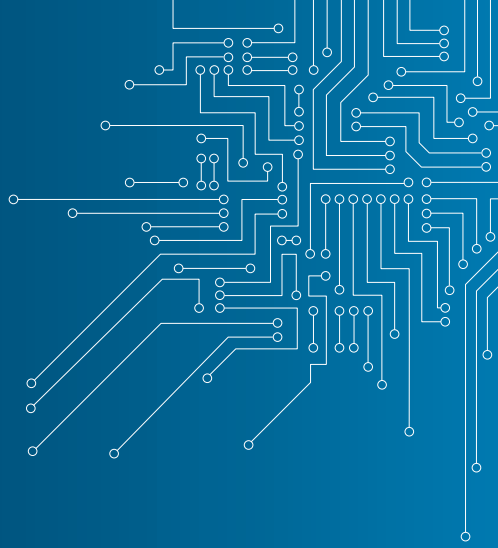




CENTRE FOR  
**CYBER SECURITY**  
BELGIUM



CYBER SECURITY  
**COALITION**.be



---

**CENTRE FOR  
CYBER SECURITY BELGIUM**

Rue de la Loi, 16 - 1000 Brussels

T. : +32 2 501 05 63  
info@ccb.belgium.be  
www.ccb.belgium.be

.be