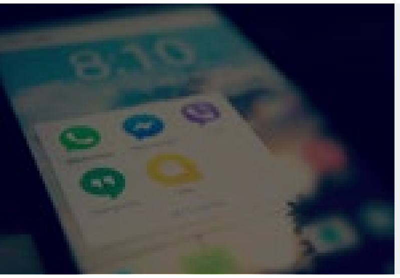
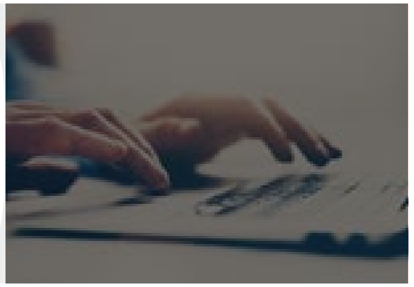
CPA Guide on Best Practices in IT Use

CHARTERED
PROFESSIONAL
ACCOUNTANTS
BRITISH COLUMBIA

TABLE OF CONTENTS





SELF-DIAGNOSIS OF YOUR PRACTICES 1/3

- PERFORM A SELF-DIAGNOSIS TO ASSESS THE EXTENT TO WHICH YOUR INFORMATION TECHNOLOGY PRACTICES ARE CURRENT AND CONSULT THE FOLLOWING GUIDE TO HELP YOU ADOPT SAFE, BEST PRACTICES.

Does a question resonate with you? Click here and follow the guide.

Is your workstation protected by a user name and password?

Are the passwords sufficiently secure?

Does your workstation automatically switch to sleep mode after a certain period of time?

Is the user name and password to access your workstation shared or stored in a location that is accessible to a member of your firm or your employer in the event of death or sudden incapacity?

Is your workstation protected by anvirus software that is updated automatically?

Are hard disks on laptops encrypted?

Do you offer your staff or does your employer offer an employee training and awareness program on security policies, guidelines and procedures?

Are these policies, guidelines and procedures communicated to staff?

When an employee leaves, are his or her accesses to the server, accounts and documents removed in order to ensure data confidentiality?

Have you set up a method to manage backups of data (information related to your clients) stored on your network?

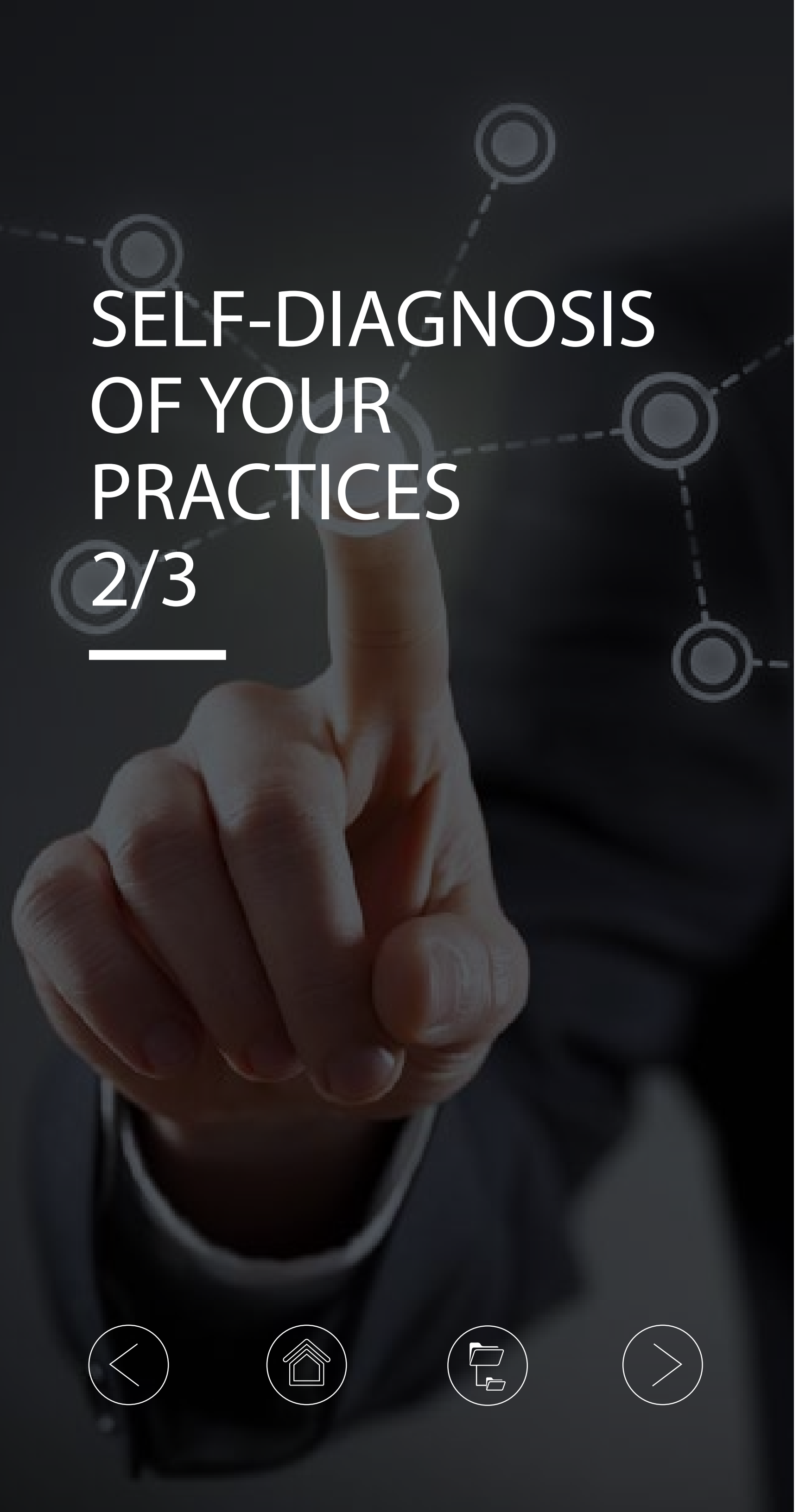
Do you know how often data is backed up?

Do you know where the backup copies are stored?

Are the backup copies encrypted or protected by an adequate password?

Do you know if stored data can be recovered in a readable format so as to be consulted in the short term?

Continue your self-diagnosis



SELF-DIAGNOSIS OF YOUR PRACTICES 2/3

Is the data housed in a hosted or cloud-computing environment, or on a local network?

If you use a local network, is it protected by a regularly updated firewall?

Is the physical security of this server ensured?

If visitors are provided access to a network, is this network separate from the one that provides access to data?

When you do business with an external or internal consultant who may have access to data relating to your clients contained in your information system (internal network, workstation, mobile computer, smartphone, hosted and cloud-computing environment, or other), do you have the consultant sign a confidentiality agreement?

If data is hosted externally, has a contract been signed with a cloud-computing provider?

Does the contract include:

- measures to ensure the confidentiality of hosted data?
- measures to ensure the integrity of hosted data?
- measures respecting accessibility to hosted data, allowing you access at all times?
- a data destruction process and data retention measures?
- a process to recover hosted data that ensures its value and integrity?
- a data backup and retention schedule?

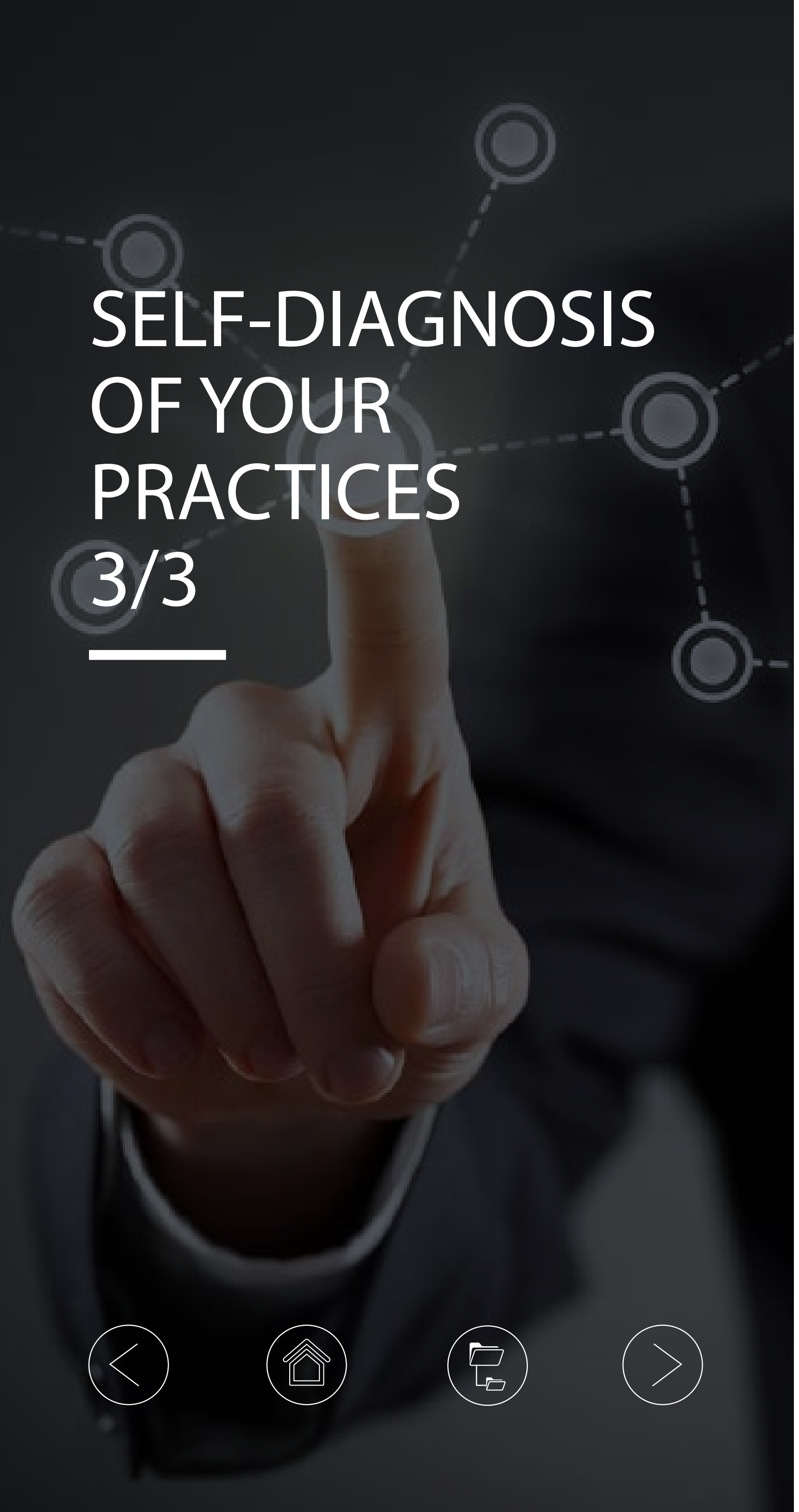
Does the contract include a clause:

- ensuring that you or your employer remain the owner of the hosted data and that the data will be destroyed at the end of the contract?
- requiring the provider to inform you in the event of data theft or breaches?
- allowing you to carry out audits or to receive the audit findings?
- respecting insurance coverage in the event of data loss?

Are clients informed that data concerning them is saved on an external server?

Is the data hosted in Canada and is the provider Canadian-owned?

Continue your self-diagnosis



SELF-DIAGNOSIS OF YOUR PRACTICES 3/3

Do you have a service platform (portal or file exchange) that is accessible to your clients? If so, have you implemented measures to ensure its security?

If you communicate with your clients or employer by email, do you know whether the service you use guarantees privacy and uses an encryption system?

Do you encrypt messages and documents sent by email?

Do you obtain authorization from your clients before exchanging confidential information via email with them?

If you use text messaging to send confidential information, how do you ensure that the information remains confidential?

Does your smartphone contain data about your clients or belonging to your employer?

Is data saved on mobile platforms (laptops, tablets, USB keys, external hard drives, etc.) sufficiently protected and even encrypted?

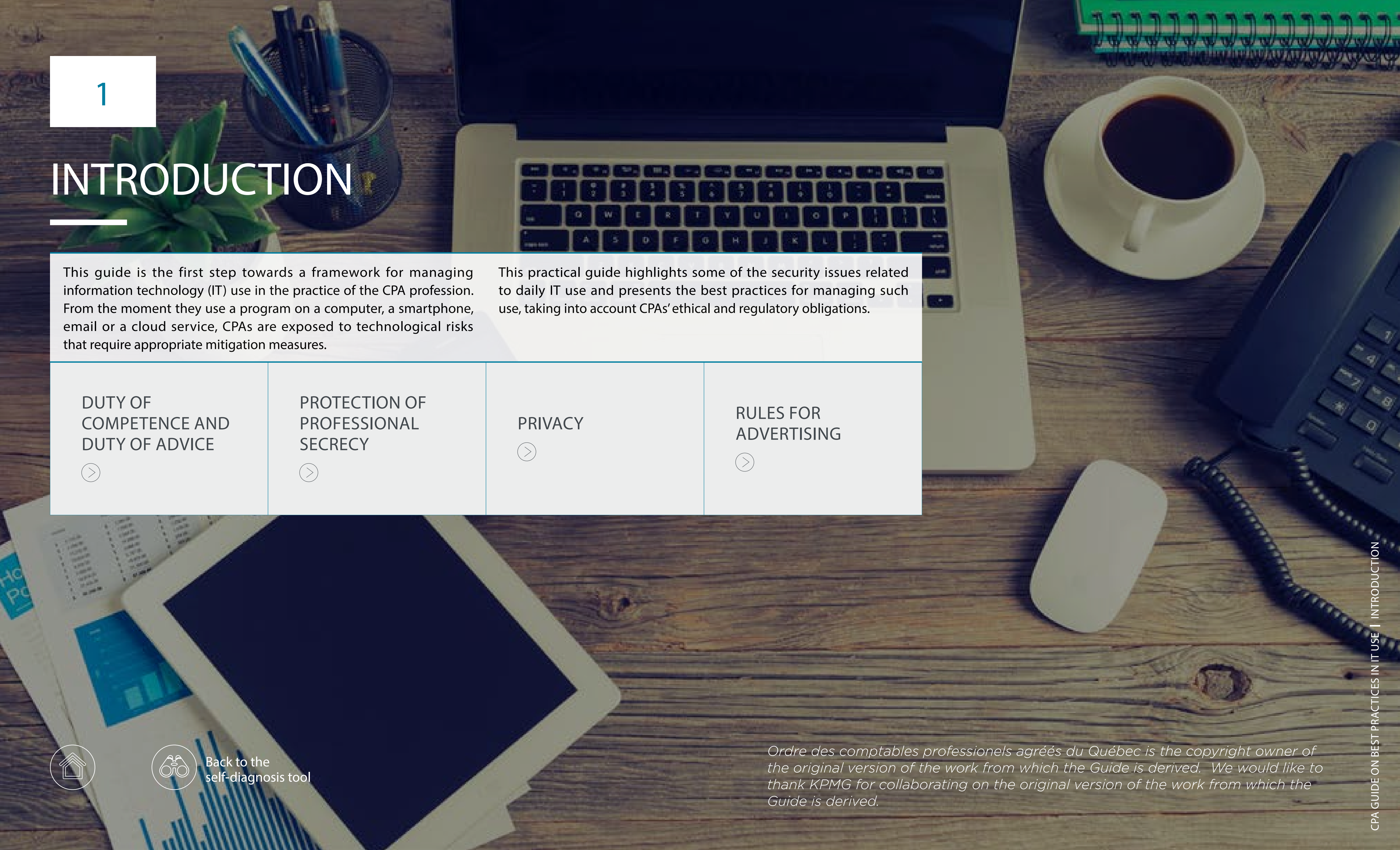
Do you sometimes use unsecured public networks with a mobile platform containing data about your clients or employer?

Do you allow your employees, or does your employer allow you, to use personal devices, and if so, do these devices have to comply with security requirements (up-to-date antivirus software, data encryption, and passwords that are robust and changed frequently)?

Has a policy been implemented on the use of these technologies and the required security measures?

Do you have sufficient security safeguards for employees who connect remotely (e.g. VPN access)?

When remote access is used, from home for instance, how do you ensure that the home's Internet network is secure and that professional data is not accessible?



1

INTRODUCTION

This guide is the first step towards a framework for managing information technology (IT) use in the practice of the CPA profession. From the moment they use a program on a computer, a smartphone, email or a cloud service, CPAs are exposed to technological risks that require appropriate mitigation measures.

This practical guide highlights some of the security issues related to daily IT use and presents the best practices for managing such use, taking into account CPAs' ethical and regulatory obligations.

DUTY OF COMPETENCE AND DUTY OF ADVICE

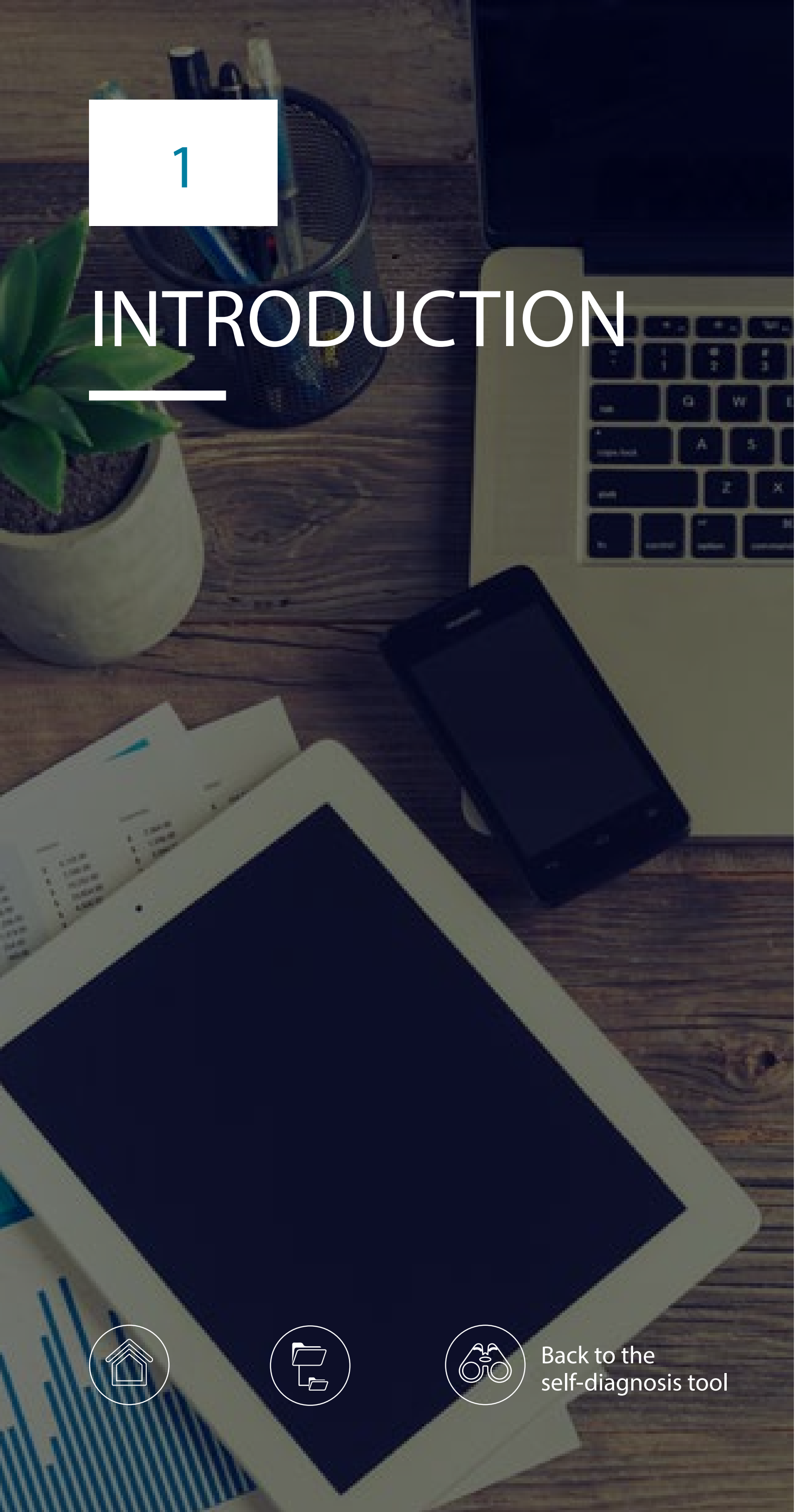
PROTECTION OF PROFESSIONAL SECRECY

PRIVACY

RULES FOR ADVERTISING

Back to the self-diagnosis tool

Ordre des comptables professionels agréés du Québec is the copyright owner of the original version of the work from which the Guide is derived. We would like to thank KPMG for collaborating on the original version of the work from which the Guide is derived.



1

INTRODUCTION

Back to the self-diagnosis tool

Duty of competence and duty of advice

Like all professionals, CPAs have a general duty of competence. They must therefore have acquired extensive knowledge that goes beyond an understanding of accounting rules and includes the ethical requirements related to the practice of the profession. Whether they offer services to third parties or not, CPAs must keep abreast of developments in the fields in which they practice their profession and maintain their competence in these areas. Part of CPAs' duty of competence is a duty of advice towards their clients, who may be their employer.

Protection of professional secrecy

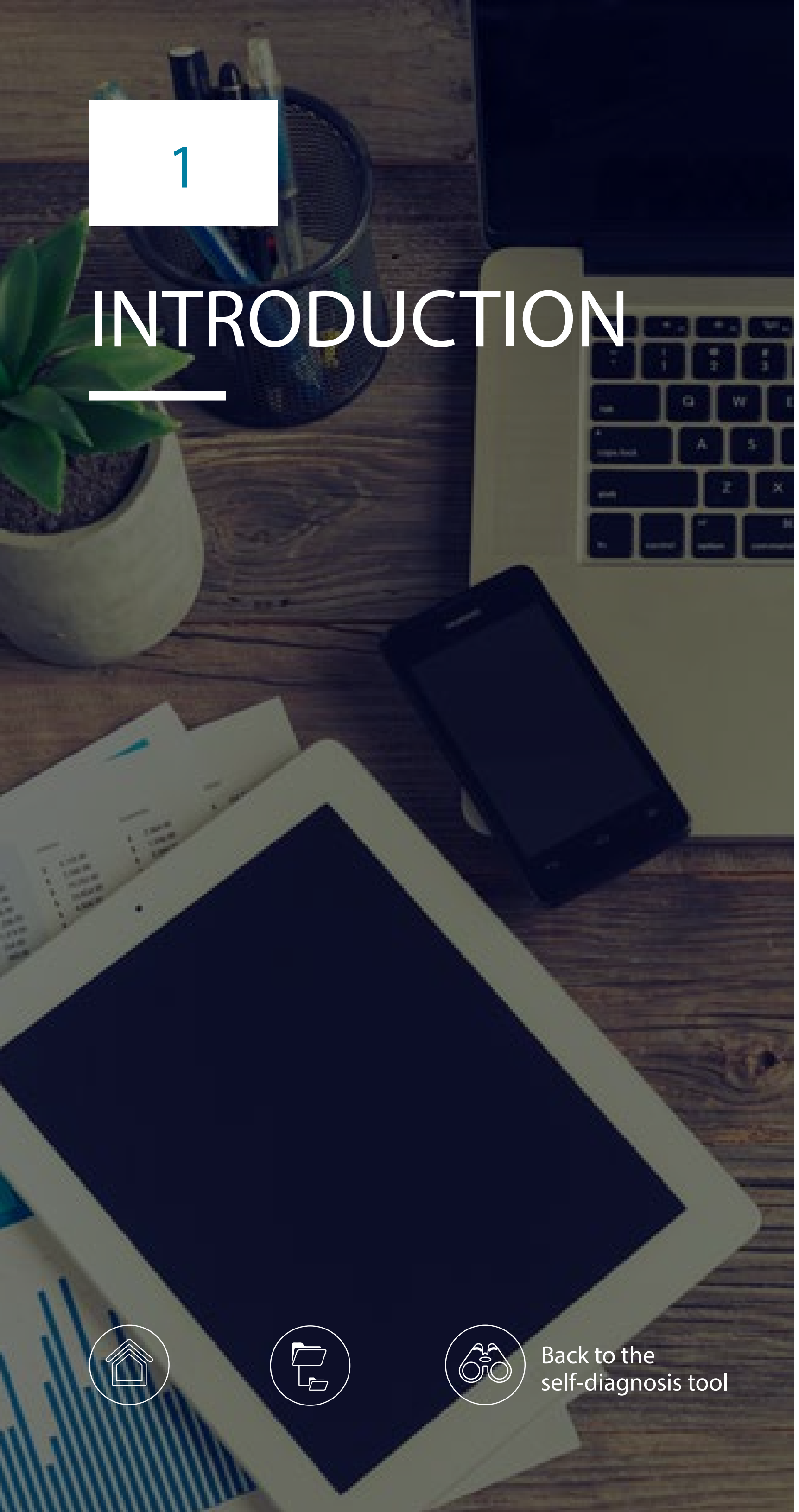
All CPAs are bound by professional secrecy. They may not disclose confidential information revealed to them by reason of their profession, unless they are authorized by the person who confided the information to them (their client) or by an express provision of law. Professional secrecy is a right provided for under the Professional Code and the Code of ethics of CPAs. This right is also recognized by the Charter of human rights and freedoms, which requires compliance from all professionals.

IT use can have a direct impact on professional secrecy. Therefore, CPAs need to understand their obligations and the sensitive nature of the information in their possession in order to prevent inadvertent disclosure when they store, transfer or destroy such information. CPAs must protect confidentiality, whether the information is in paper or electronic form, ensuring that only authorized persons can access it. This guide identifies several situations where access points may become vulnerable and proposes mitigation measures.

Solo practice of the profession and the use of paper records limit exposure to confidentiality risks. Conversely, the number of collaborators, modes of collaboration and use of networks (mobile, internet, applications and remote servers) redefine the security perimeter. The number of access points to control increases as a result.

CPAs would never have a meeting in a public place where they could be seen or heard. The same discretion should also be applied online, which requires an understanding of information security concepts and the environment the CPA intends to use.

In practice, this means CPAs have to be able to identify at-risk situations and inform their clients when faced with a risk stemming from IT use (for example, email communications).



1

INTRODUCTION

Back to the self-diagnosis tool

Privacy

In addition to respecting their clients' right to professional secrecy, CPAs must protect the personal information they receive (e.g. social insurance number, date of birth), regardless of the medium or format used to record or access the information (written, graphic, audio, visual, computerized or other). CPAs must protect personal information against intrusion and, except as provided for by law, may only communicate it to third parties with their client's consent.

In practice, CPAs are required to:

> Protect the information entrusted or accessible to them against any potential breach of confidentiality by ensuring the environment is secure.

> Have at least a basic understanding of the technology features they use depending on whether the messages are public or private.

> Recognize situations that threaten information security.

> Adopt appropriate measures to mitigate these risks.

> Be aware of their limitations in knowledge and skills, and consult specialists as needed to secure their servers.

> Obtain their clients' consent before transferring information to third parties or using information exchange technology.

> Inquire into technological advances and ensure their solutions are appropriate and up to date.

> Store and access Personal Information only in Canada where British Columbia's Freedom of Information and Protection of Privacy Act (FOIPPA) applies, unless expressly permitted under FOIPPA.

Rules for advertising

CPAs are subject to advertising rules. They may not confer or have conferred upon themselves specific qualities or skills regarding, for example, their level of competence or the extent of their services, unless these can be supported. They should therefore exercise caution and weigh the words they post on their websites or social media, to avoid misleading the public about their competence or that of their firm. They also cannot use or allow the use of advertising that is false, misleading, incomplete, or derogatory to the honour or dignity of the profession.

These obligations apply regardless of the medium used. Since CPAs' websites (or social media profiles) are promotional tools (therefore tools they manage), comments posted by third parties could put CPAs in violation of their obligations.

CPAs should moderate third party comments and correct them if necessary before they are published in an environment they control. Where this is not possible, CPAs should regularly screen the comments after they have been published.

2

INFORMATION SECURITY PRINCIPLES

KEY PRINCIPLES

CRITICAL INFORMATION ASSET PROTECTION

Back to the
self-diagnosis tool

2

INFORMATION SECURITY PRINCIPLES

› KEY PRINCIPLES

Availability, integrity and confidentiality are the key principles of information security.

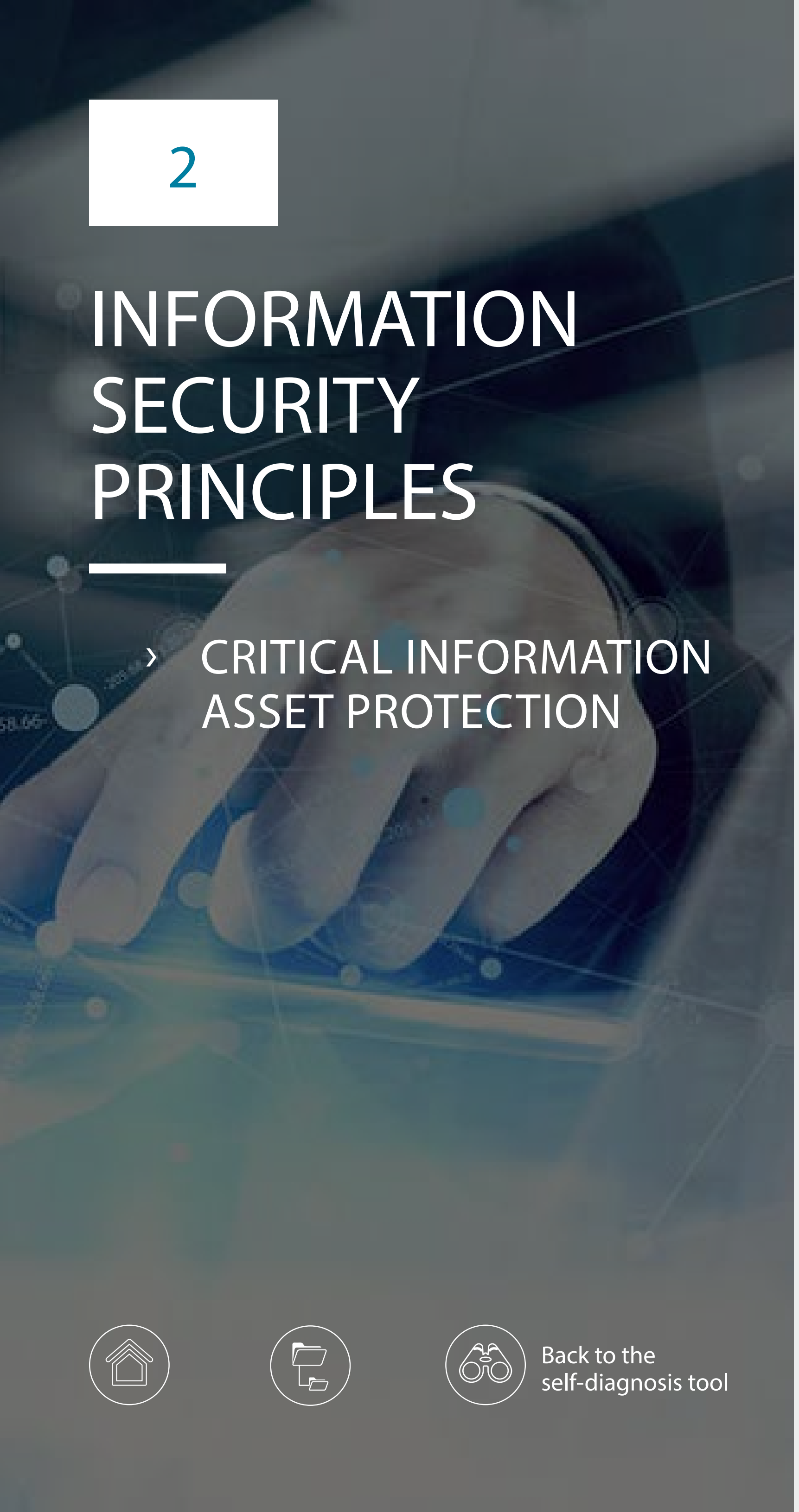
Availability means that information capital is accessible to all authorized users in a timely manner. Internet access failure – be it accidental or due to a Denial of Service (DoS) attack – can hold up or block commercial or professional activities. A ransomware attack (malicious software that encrypts files and demands ransom for the decryption key) can also slow down or halt activities.

Integrity is the assurance that documents or records have not been altered or redacted since their creation. This criterion is fundamental in British Columbia law for a document to be admissible as evidence before a decision-making body.

Integrity goes hand in hand with traceability. Traceability ensures that the history of information can be recreated and traced. Simple and free utilities can determine whether a document has been altered (voluntarily or not) by comparing the hash value of the communication received to the hash value of the communication sent.

Confidentiality should be protected when a document is stored or sent. Therefore, protection and risk management measures should be implemented. To preserve the confidentiality of an attachment to an email sent over an unsecured connection, encrypt the document and provide the recipient with the password over the phone or in a separate email. An even more effective measure is to place the document on a secure sharing platform and notify the recipient that it is available for download.

Back to the
self-diagnosis tool



2

INFORMATION SECURITY PRINCIPLES

› CRITICAL INFORMATION ASSET PROTECTION

Back to the self-diagnosis tool

Identifying the information assets that require protection is an important step in implementing a security framework. To this end, the criticality level of these information assets must be defined based on the three security principles: availability, integrity (which includes traceability) and confidentiality. Critical information assets include the following:

> Information protected by professional secrecy or covered by privacy legislation

> The processes and methods developed to deliver services

Information assets may be subject to various types of threats:

> Human (hacking, data theft)

> Natural (floods, solar storms, earthquakes)

> Technical (bugs)

> Physical (breakage, obsolescence)

BEST PRACTICES

> Instill a strong information security culture by increasing awareness and informing employees of the risks to which they are exposed.

> Identify critical information assets.

> Periodically assess information security risks.

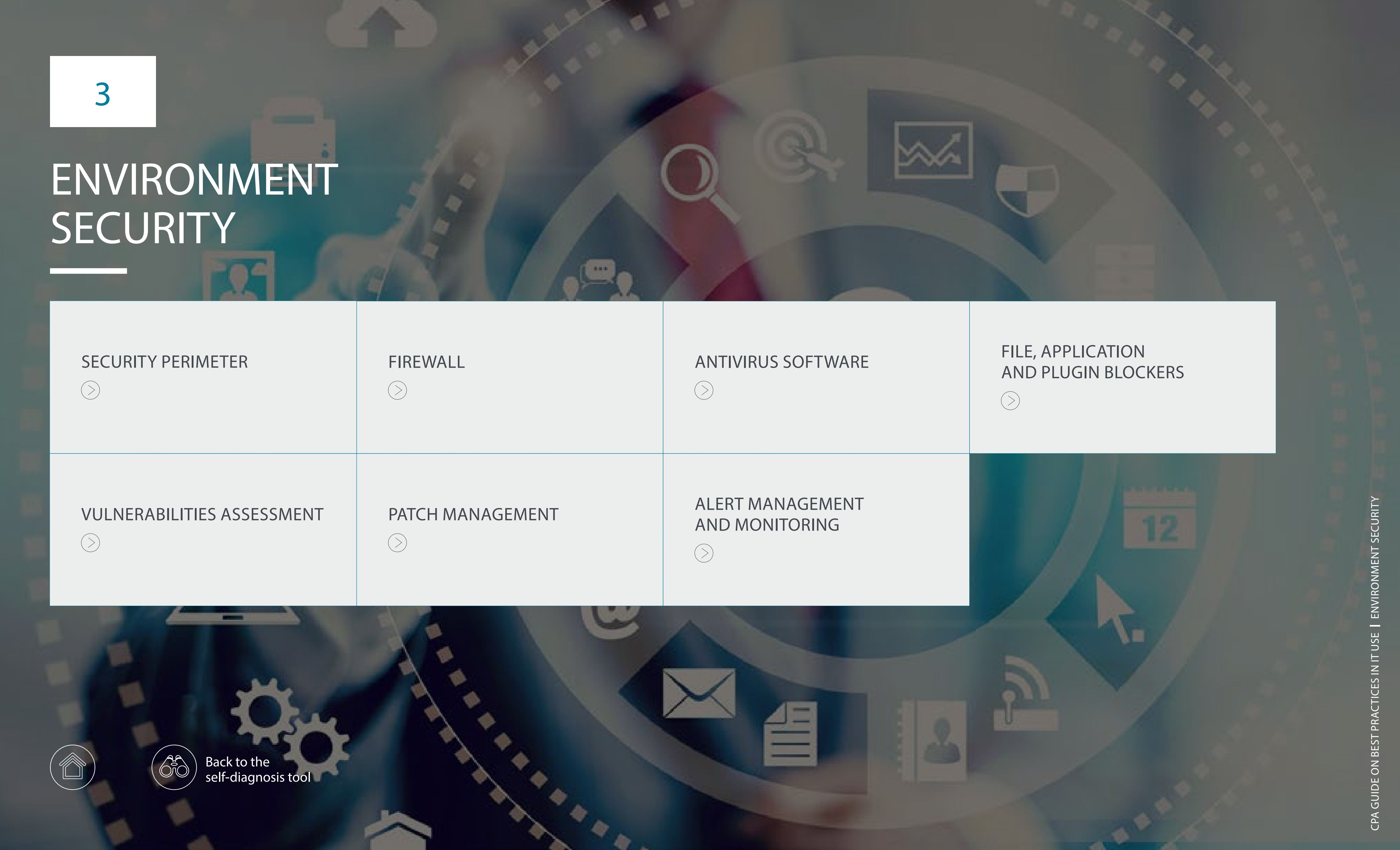
> Determine which security mechanisms are necessary to reduce the organization’s vulnerability to an acceptable level.

> Document actions, evaluate their effectiveness and implement appropriate corrective measures.

> Implement a risk-management process (guidelines, procedures and processes) associated with the information lifecycle: creation, use, storage, sharing and destruction.

> Ensure the established framework is applied (e.g. audits, annual certification).

> Consider cyber liability insurance.



3

ENVIRONMENT SECURITY

SECURITY PERIMETER

FIREWALL

ANTIVIRUS SOFTWARE

FILE, APPLICATION AND PLUGIN BLOCKERS

VULNERABILITIES ASSESSMENT

PATCH MANAGEMENT

ALERT MANAGEMENT AND MONITORING

Back to the self-diagnosis tool

3

ENVIRONMENT SECURITY

› SECURITY PERIMETER

Back to the
self-diagnosis tool

The concept of security perimeter is important because it delineates the scope of the measures needed to protect information effectively.

The security perimeter of an unconnected computer is limited to the one room in which it is located. If a computer is connected to a server in another room, the perimeter extends to this other room, which then needs to be secured in some way (a security guard, lock). If the connection is wireless, the signals need to be encrypted, that is, made unintelligible to unauthorized parties.

The perimeter expands further to every person who works with a CPA in the practice of his or her profession. When working with external providers, CPAs must verify their confidentiality practices, and make sure the service agreement provides for information protection.

The perimeter also increases if a smartphone that contains work documents and applications for communication with clients is added to the mix. The perimeter grows based on the number of applications that, when activated, can access information stored in the device (contacts, files, history, location data, etc.). For example, activating positioning (e.g. with GPS) could reveal the name of a client to an application on the device.

3

ENVIRONMENT SECURITY

› FIREWALL

A firewall is used to protect a computer system against attacks from another. The firewall creates trusted zones by separating requests from the local network and requests from the external network. The firewall then monitors and controls incoming and outgoing network traffic and based on a set of security rules determines whether the traffic is permitted or blocked.

BEST PRACTICE

> Install a firewall, configure it properly based on the organization's needs, and keep it up to date. It may be necessary to consult networking professionals, depending on the network's complexity (Is there an extranet? Virtual private network? Web or email servers?) and the size of the organization.

Back to the self-diagnosis tool

3

ENVIRONMENT SECURITY

› ANTIVIRUS SOFTWARE

Sophisticated viruses and other malware (malicious code) have made antivirus and anti-malware software a must. These software help protect against illicit acts such as:

- Exfiltrating data
- Blocking access to information, then extorting the victim for its retrieval
- Tricking victims using more or less sophisticated schemes. For example, sending malware to someone who holds a specific position in an organization, leading the victim to open an attachment from an unknown source, such as a fake delivery receipt through a private messaging system. A scheme can also involve luring users to click on a link to an infected site (often following a phishing attack and sometimes targeting a specific person) or to plug in an unknown removable medium, like a USB flash drive containing malicious software.

BEST PRACTICES

- Install antivirus and anti-malware software, configure it properly, preferably with automatic updates.
- Make employees aware of the different types of computer threats. A human action usually spreads viruses and malware.

Back to the self-diagnosis tool

3

ENVIRONMENT SECURITY

› FILE, APPLICATION AND PLUGIN BLOCKERS

Back to the self-diagnosis tool

Viruses and other malware are spread through known vectors that are relatively easy to block. Attachments that have executable files (files that contain a program directly executable by the processor and that enable the launch of an application or a command) or files with executable code (e.g. macros) must be blocked or at least disabled until the user activates them within an application. For example, certain functions in a file, such as macros, can only be activated by the user, who confirms that the attachment comes from a reliable source beforehand.

BEST PRACTICES

- When configuring email servers, block executable or compressed attachments (*.exe, *.bat, *.msi, .zip, .rar, etc.).
- Configure the spam filters to block phishing attempts and malicious attachments.
- By default, deactivate macros and other executable code in files that may contain them: word processing software, spreadsheets, databases, PDF files, etc.
- Warn staff not to open files or activate macros unless they trust the sender.
- Block applications and plugins known for their information security weaknesses, even if they are frequently updated (Flash, Java, search bars, wallpaper, etc.).
- Stay current on these kinds of threats and ensure employees are aware of any developments.

3

ENVIRONMENT SECURITY

› VULNERABILITIES ASSESSMENT

Back to the self-diagnosis tool

When an organization implements security measures it considers reasonable, its exposure to risk reduced but not eliminated. An information security specialist should therefore conduct a vulnerability assessment at regular intervals. This measure is used to evaluate a system's capacity to block hacking attempts varying in sophistication. The measure also documents identified vulnerabilities in order to address them.

BEST PRACTICES

- Regularly conduct logical penetration tests (system security, phishing simulation, etc.).
- Occasionally conduct physical penetration tests (entry into the workplace, the copy/mail/server room, etc.).
- Conduct social engineering tests (obtain useful information such as passwords, install software executed by an email, pose as an executive to make an emergency transfer, etc.).

3

ENVIRONMENT SECURITY

› PATCH MANAGEMENT

Back to the self-diagnosis tool

Patches correct software vulnerabilities and update hardware and software in the organization’s computer system.

While it is recommended to enable automatic updates for security software (firewall, antivirus, etc.), it is best to check first whether the updates for other kinds of software are compatible with the system in place. Update issues with major publishers are rare and usually addressed quickly. However, with others, the updates may require fixes more often, in which case the publisher should be contacted.

BEST PRACTICES

- Keep an inventory of the hardware and software used in the organization and their updates.
- Where possible, configure the applications so available patches are brought to the system administrator’s attention, and not installed automatically.
- However, enable automatic patches for security applications that monitor the signatures of malicious code or viruses to address new vulnerabilities quickly.
- Test critical applications in a separate environment to ensure updates are compatible before they are operational.

3

ENVIRONMENT SECURITY

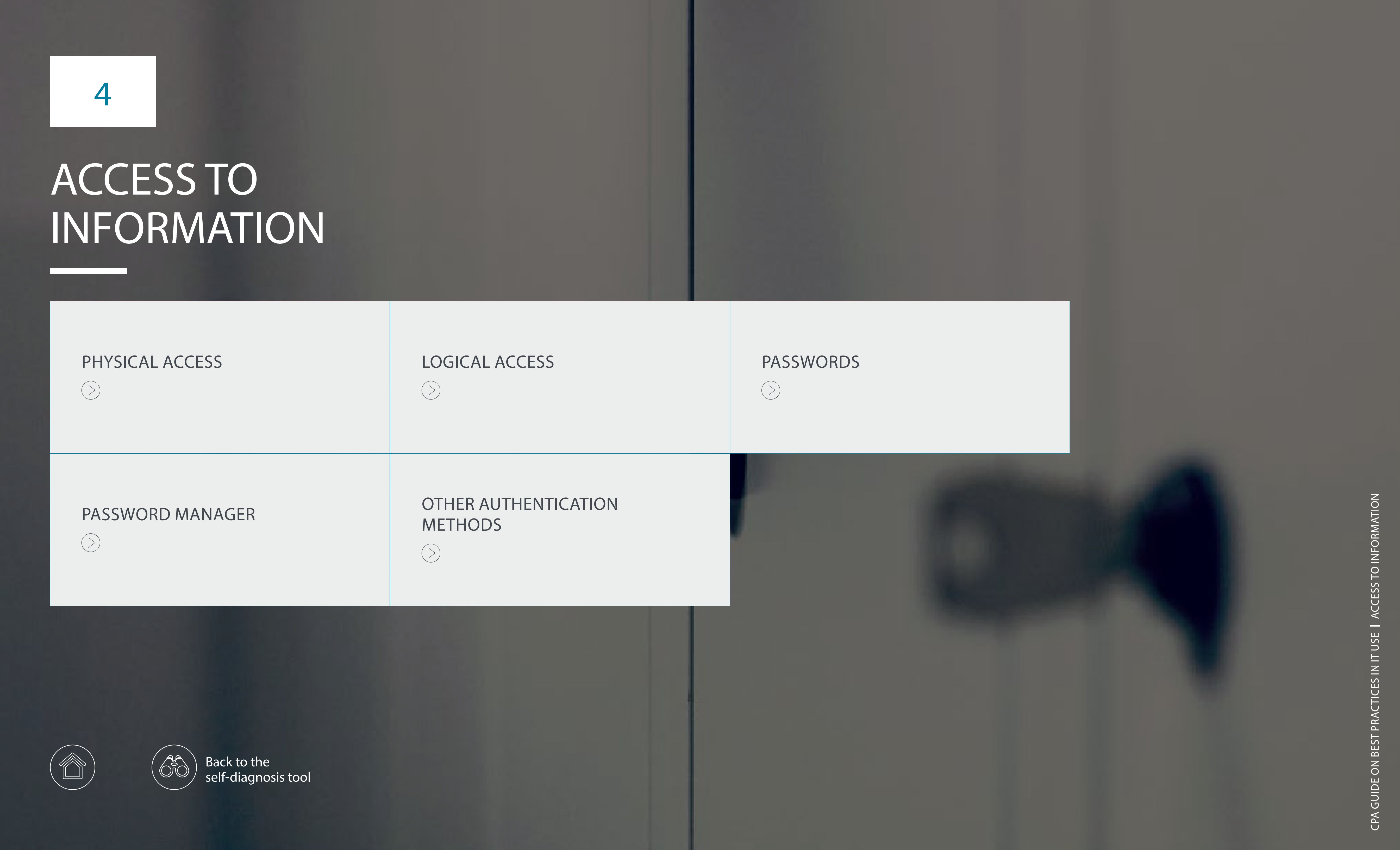
› ALERT MANAGEMENT AND MONITORING

Back to the self-diagnosis tool

The security perimeter and internal systems are monitored by software tools that detect abnormal situations, for example penetration attempts from suspicious sources. The data collected in the logs or the configuration parameters of the network protection tools are then compared against reference standards. An alert signals the presence of a potential issue, if any.

BEST PRACTICES

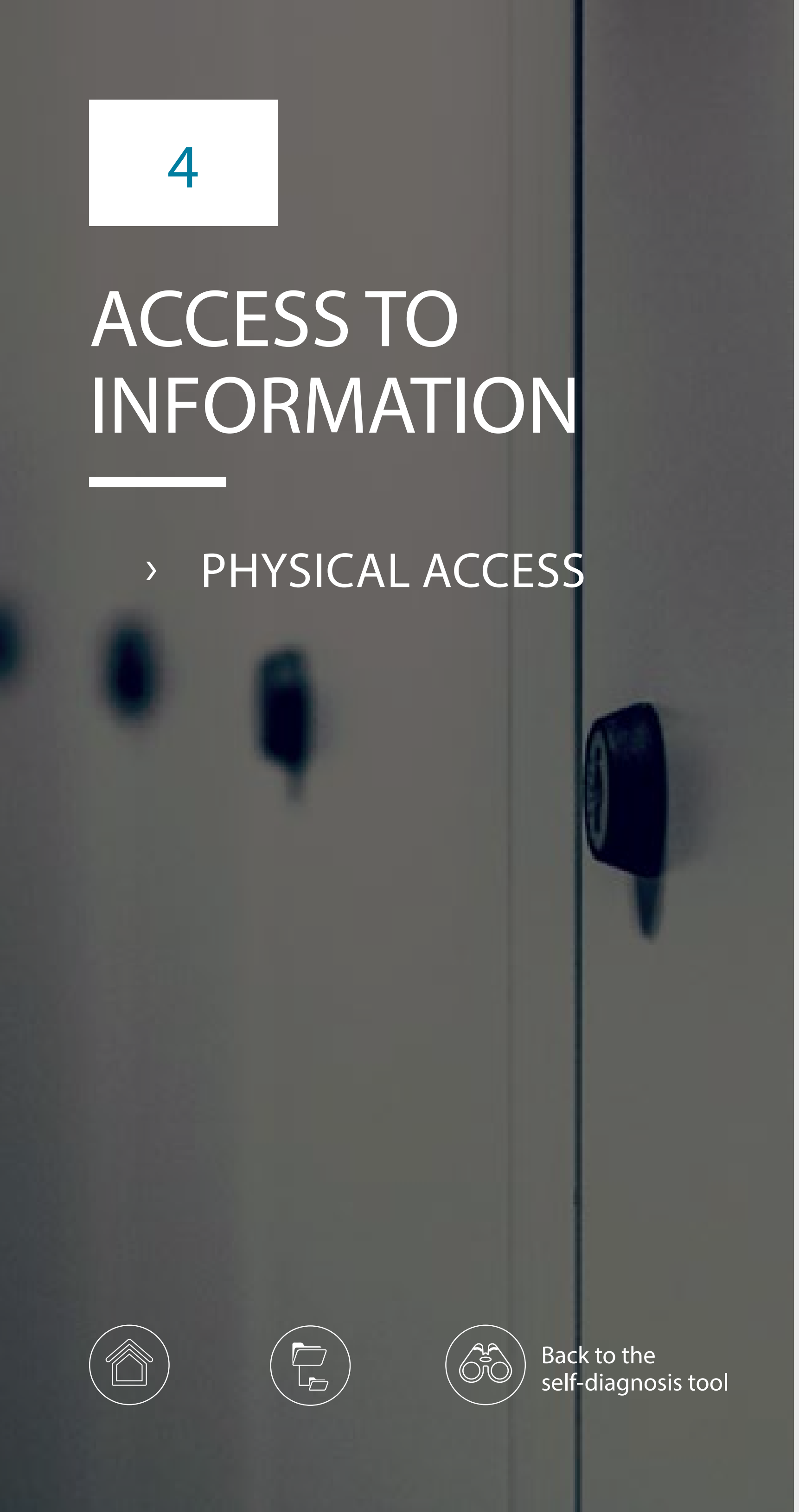
- Understand how alerts work in the various systems used.
- Follow up on alerts when they are generated.
- Document or otherwise keep track of alerts and follow-up measures to demonstrate the organization’s diligence with respect to information security and to detect longer-term trends.



4

ACCESS TO INFORMATION

Back to the self-diagnosis tool



4

ACCESS TO INFORMATION

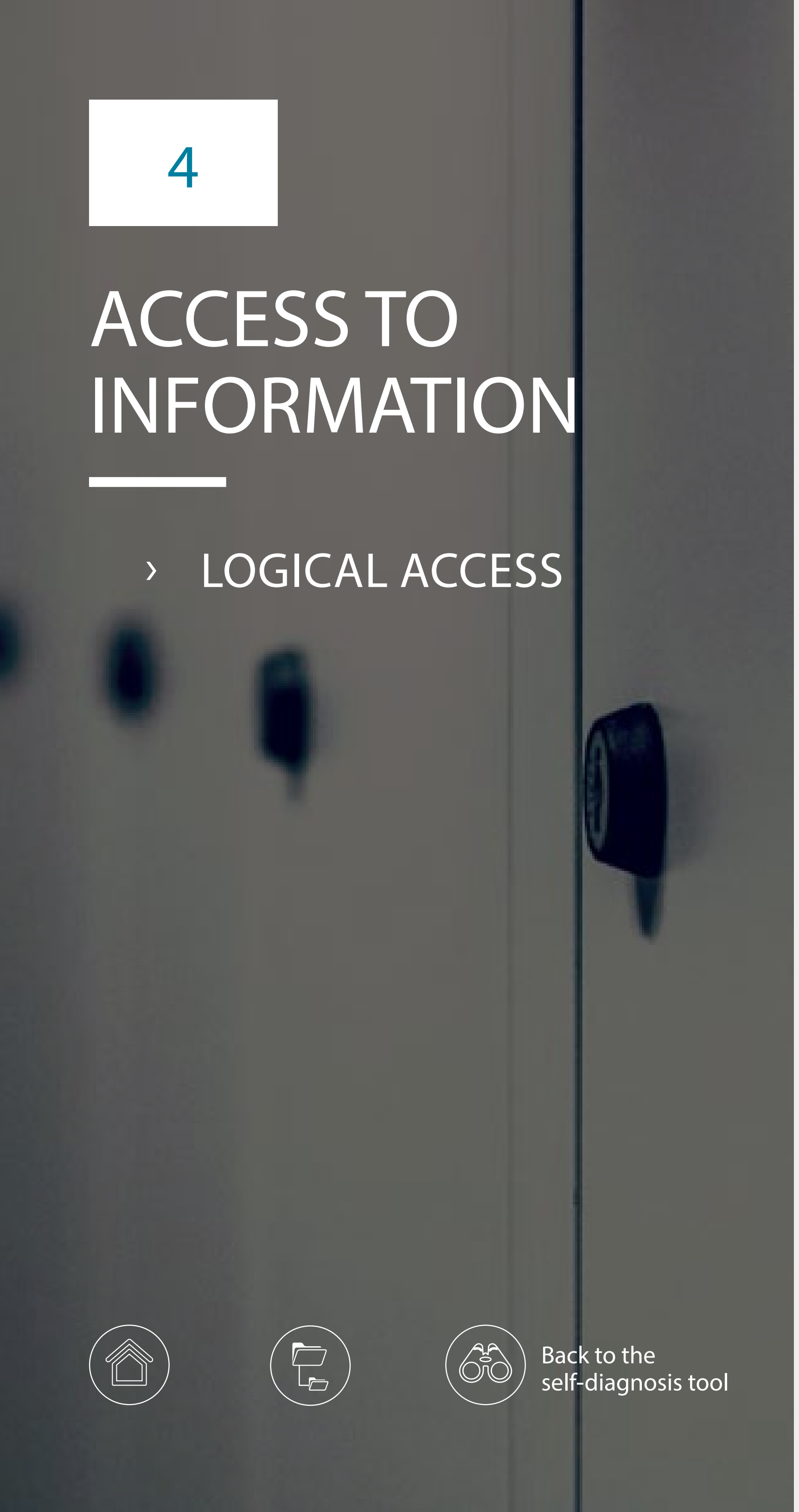
› PHYSICAL ACCESS

Back to the self-diagnosis tool

To limit the risks of someone hearing, seeing or physically taking possession of confidential information, physical access to an organization's premises must be secured, including conference, consultation, mail, copy or server rooms, and offices.

BEST PRACTICES

- Lock all offices and rooms.
- Keep track of all keys and magnetic cards in use.
- Never store magnetic keys with business cards or any other item giving the location of the workplace.
- Urgently report all lost or stolen magnetic cards to the designated person in charge.
- Equip screens used in environments accessible to third parties with polarized protective filters (privacy screens) to limit the field of vision.
- Control client and visitor access and accompany them in workspaces.
- Accompany all clients and visitors in server rooms. Also, keep logs of who enters and exits these locations.
- Keep a general log of clients and visitors who enter and exit.
- Ensure staff does not leave any confidential or sensitive documents out in the open (printer, worktable, etc.).
- Ensure that staff apply the control measures.



4

ACCESS TO INFORMATION

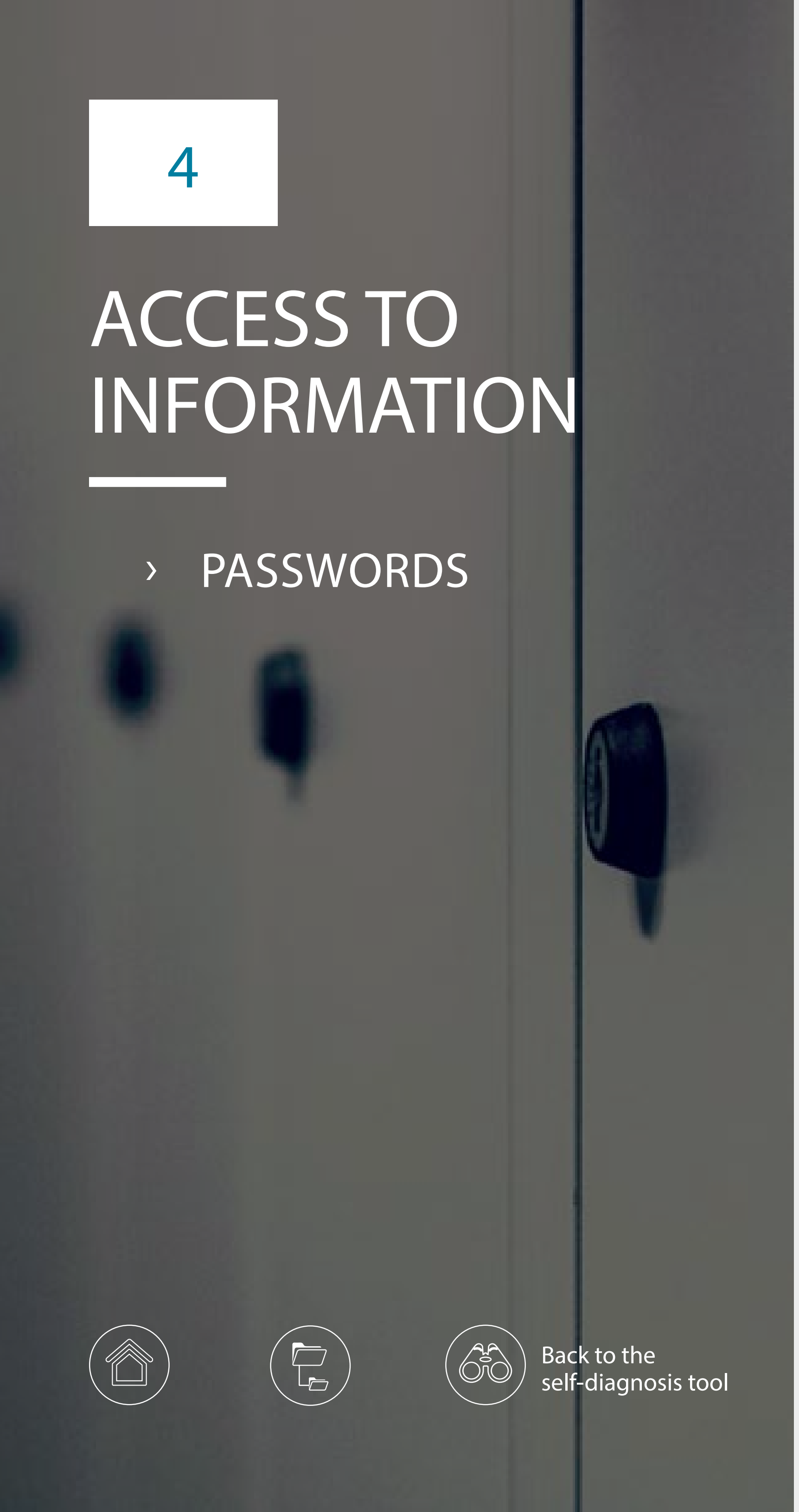
› LOGICAL ACCESS

Back to the self-diagnosis tool

Much like physical access, logical access points to data can also be limited and secured.

BEST PRACTICES

- Avoid using unsecured networks, especially in public places. Use the tools put in place by the organization to secure connections.
- Store documents in a centralized location (electronic document management system, file servers, etc.).
- Encourage employees to store documents on their computers or other portable devices for as little time as possible.
- Implement measures for secure remote access to data and applications (e.g. virtual private network, Citrix gateway or other such technologies).
- Configure computers to lock automatically after a certain time.
- Give visitors access to a network separate from the one that provides access to data.
- Implement an employee onboarding/off boarding/role change process that includes the following:
  - Procedures for changing user access rights after a role change (e.g. transfer to another department or promotion)
  - De-activation of user accounts and access permissions when an employee departs.
  - Procedures for facilitating access to files/e-mail data during the transition process.
- Use secure protocols where applicable – HTTPS, Secure FTP, IPSec, etc.
- Use encryption to encrypt disks or removable media.
- Where necessary, password-protect files that contain sensitive data.
- After a period of inactivity, disconnect idle remote access connections.
- Ensure proper access controls are in place. Limit access to data to authorized users only.
- Use multi-factor authentication where appropriate. Most of all, use multi-factor authentication to systems that are accessible via the Internet.



4

ACCESS TO INFORMATION

› PASSWORDS

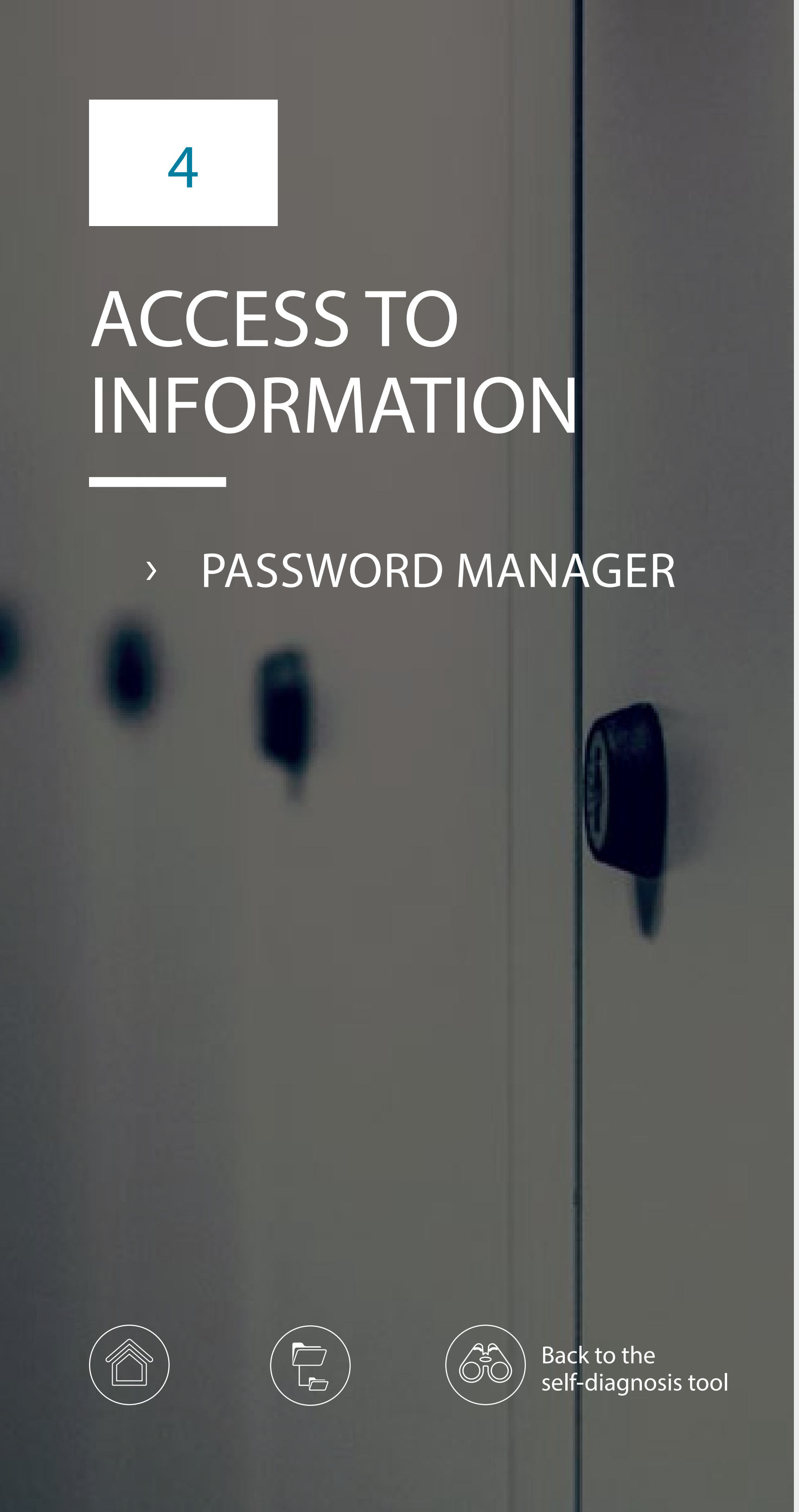
Authentication is a process by which a person or system verifies a user's identity. For passwords to be effective, they should be strong and kept secret. If a website suffers a security breach and passwords are disclosed, the passwords can be used to attempt to infiltrate other sites or systems.

With the changing threat landscape, it is becoming increasingly necessary to implement multi-factor authentication for applications that are accessible via the Internet.

BEST PRACTICES

- Never use the same password for more than one system or website.
- Use a long and complex password, (eight characters, including uppercase letters, lowercase letters, numbers, and special characters). Change it regularly and whenever you suspect it may have been compromised. However, when users change their password too often, they may be prone to create overly simple passwords. Passwords should be changed at least every three months. They should also not be reused for two years.
- Never use dates, personal information or words from the dictionary.
- Consider creating passwords using only the first letter of each word in a sentence, and insert numbers and symbols.
- Use a password manager.
- Change default user names and passwords, especially on administrator accounts (for example, on the organization's router, a prime target for hackers).
- If the system allows it, limit the number of failed attempts in order to block access.
- Have an authentication process that allows users to reset forgotten passwords.
- Manage user accounts (creation, suspension, destruction, special access) in order to limit access to authorized persons.
- Manage access rights by profile, according to the tasks and the positions held in the organization, instead of by individual, and review them periodically.
- Make sure employees with privileged access use different user names for their daily tasks and administrative roles.
- Limit, log and analyze access to critical information assets.
- Use multi-factor authentication where appropriate. Most of all, use multi-factor authentication to systems that are accessible via the Internet.

Back to the
self-diagnosis tool



4

ACCESS TO INFORMATION

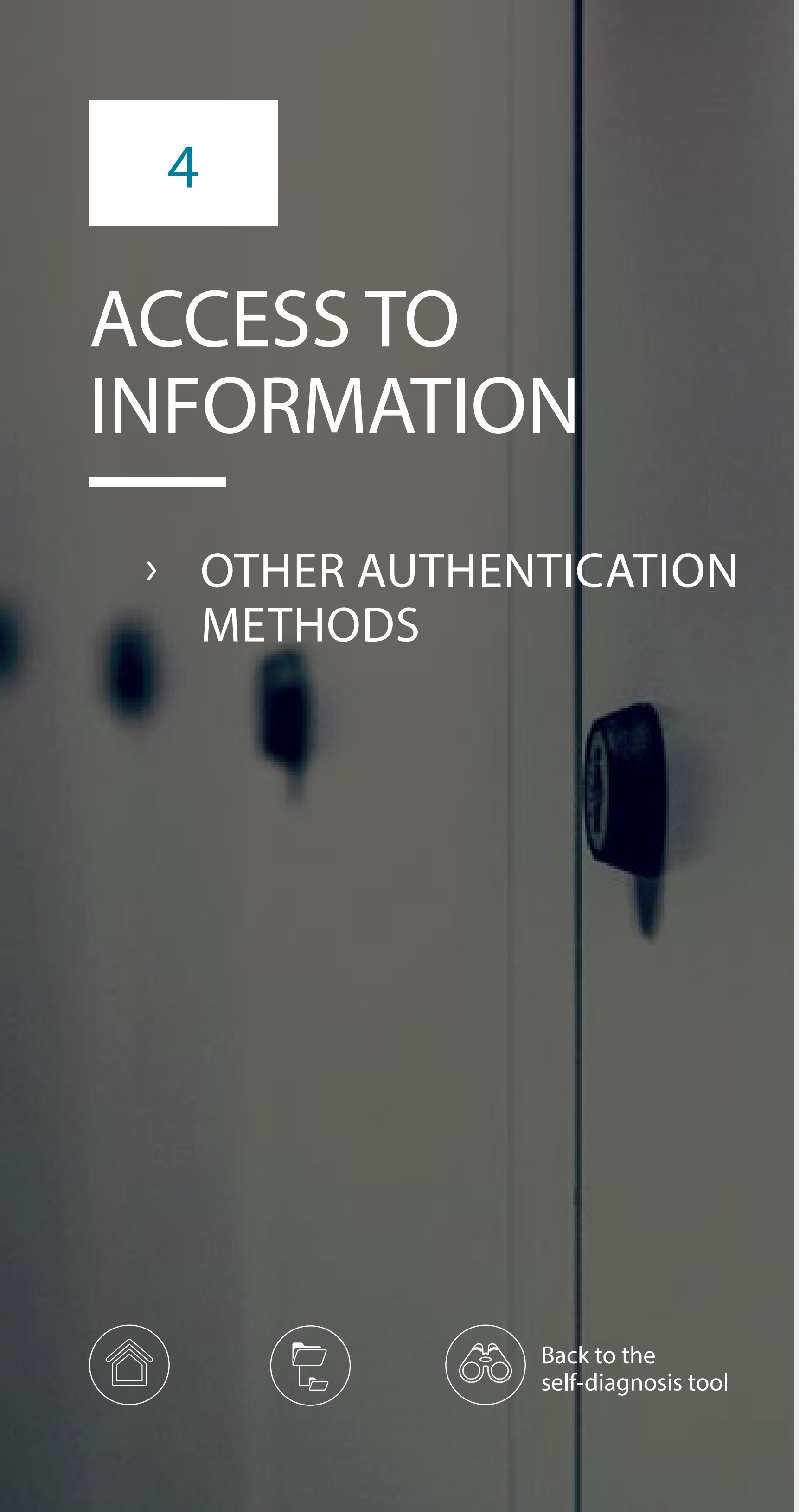
› PASSWORD MANAGER

A password management system is a database that contains all of a user's login information (user names, passwords, answers to secret questions, etc.). This database is encrypted and protected by a highly complex password of its own. The password manager can randomly generate passwords. And since users do not need to remember these passwords, it can create very long passwords that are different for each account and changed frequently.

BEST PRACTICES

- Use a password manager.
- Backup the database.
- Given the importance of the master password, have a safe way to retrieve it if needed.

Back to the self-diagnosis tool



4

ACCESS TO INFORMATION

› OTHER AUTHENTICATION METHODS

In some cases, it may be a good idea to use a two-factor authentication system to secure logical access to a system. For example, this authentication system can be used to access the organization's network remotely through the server that manages the virtual private network or a server containing critical information.

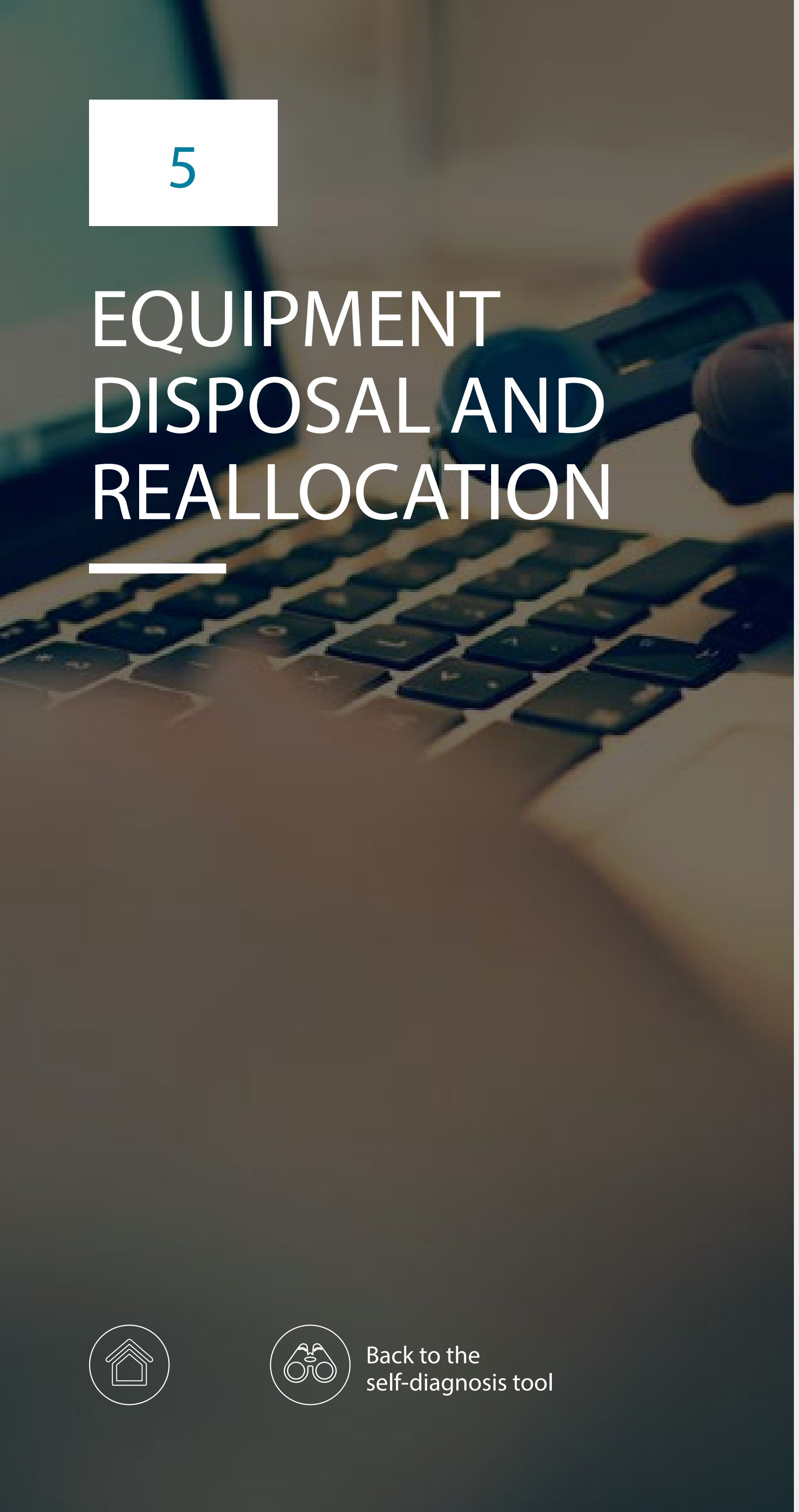
Tokens, which display a code that changes frequently, or text messages sent during the authentication process, can be a second authentication factor, after the password.

Biometrics is another form of authentication that is gaining in popularity on laptops and mobile phones. The use of biometrics reduces risks, especially those related to privacy, when the information is encrypted and stored on the device only. Risks are also diminished when one-way transformation of data is performed, thereby making it impossible, for example, to recreate a fingerprint from saved information.

BEST PRACTICES

- Activate two-factor authentication on systems that support the option, in particular on virtual private networks.
- Use biometric measures (mainly fingerprints) as an authentication method.

Back to the self-diagnosis tool



5

EQUIPMENT DISPOSAL AND REALLOCATION

A computer device or medium should no longer contain any information when it is disposed of in order to prevent a breach of the organization's security perimeter.

The data on a computing device or a data medium, such as a multifunction printer that contains a hard drive that may still have confidential information saved in the internal memory, should be destroyed before it is reassigned to another employee, donated to a charitable organization or returned to its lessor. Simple formatting is not enough, as the information may be retrievable.

BEST PRACTICES

> Use appropriate software tools to destroy data.

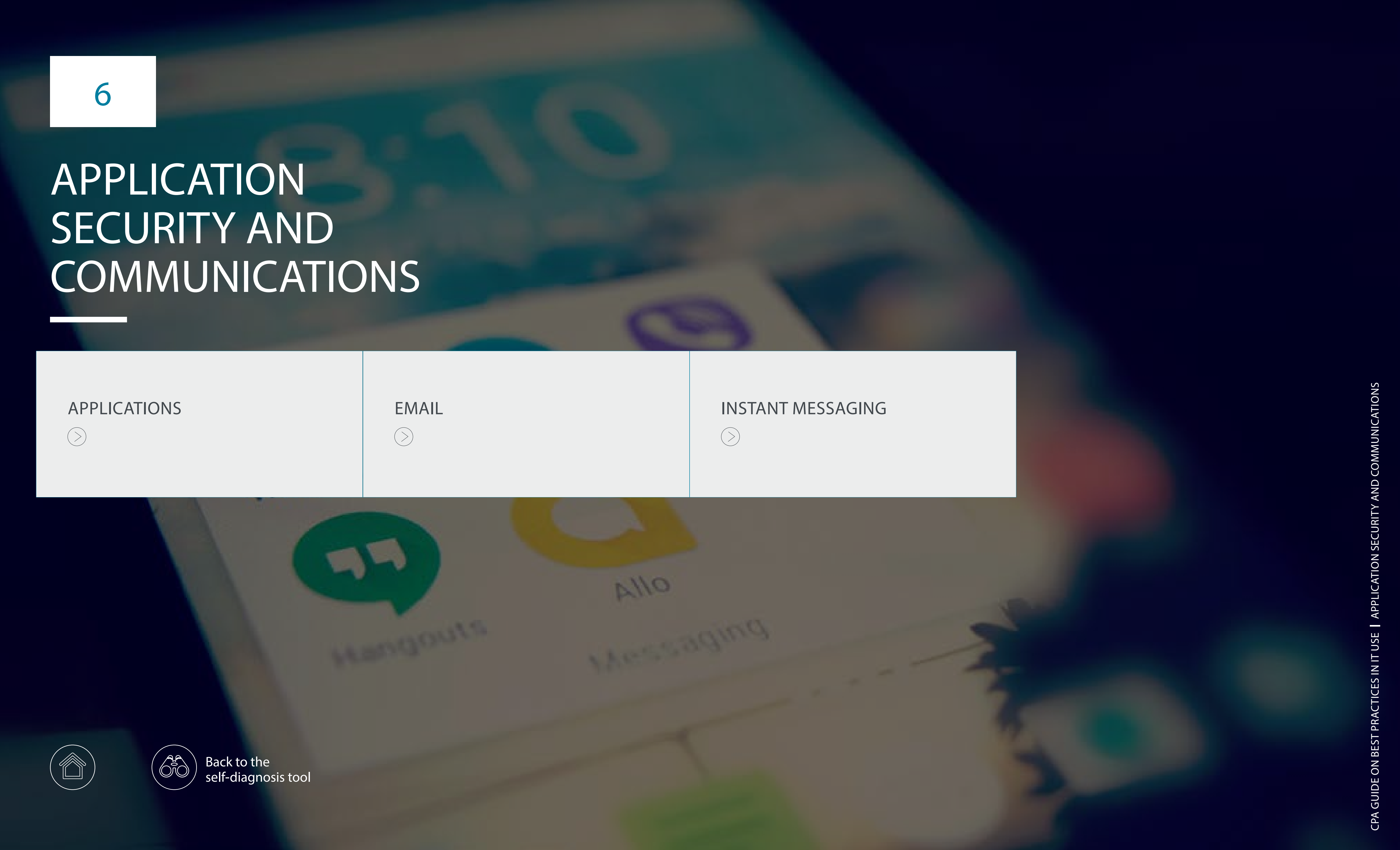
> A factory reset of telephones and tablets may be sufficient. But with the rapid evolution of data retrieval methods and tools, new measures may be required to ensure data is destroyed.

> Destroy the data on a medium before disposing of it. Easy-to-use data destruction software tools for various media are available on the market. The services of a secure data destruction provider can also be used.

> For leased devices, ensure the lessor destroys the data on the hard drives. If you are authorized, destroy the data yourself.

> When an employee leaves, retrieve all hardware and reassign the accounts (LinkedIn, Facebook, Twitter) belonging to the organization.

Back to the self-diagnosis tool



6

APPLICATION SECURITY AND COMMUNICATIONS

APPLICATIONS

EMAIL

INSTANT MESSAGING

Back to the self-diagnosis tool

6

APPLICATION SECURITY AND COMMUNICATIONS

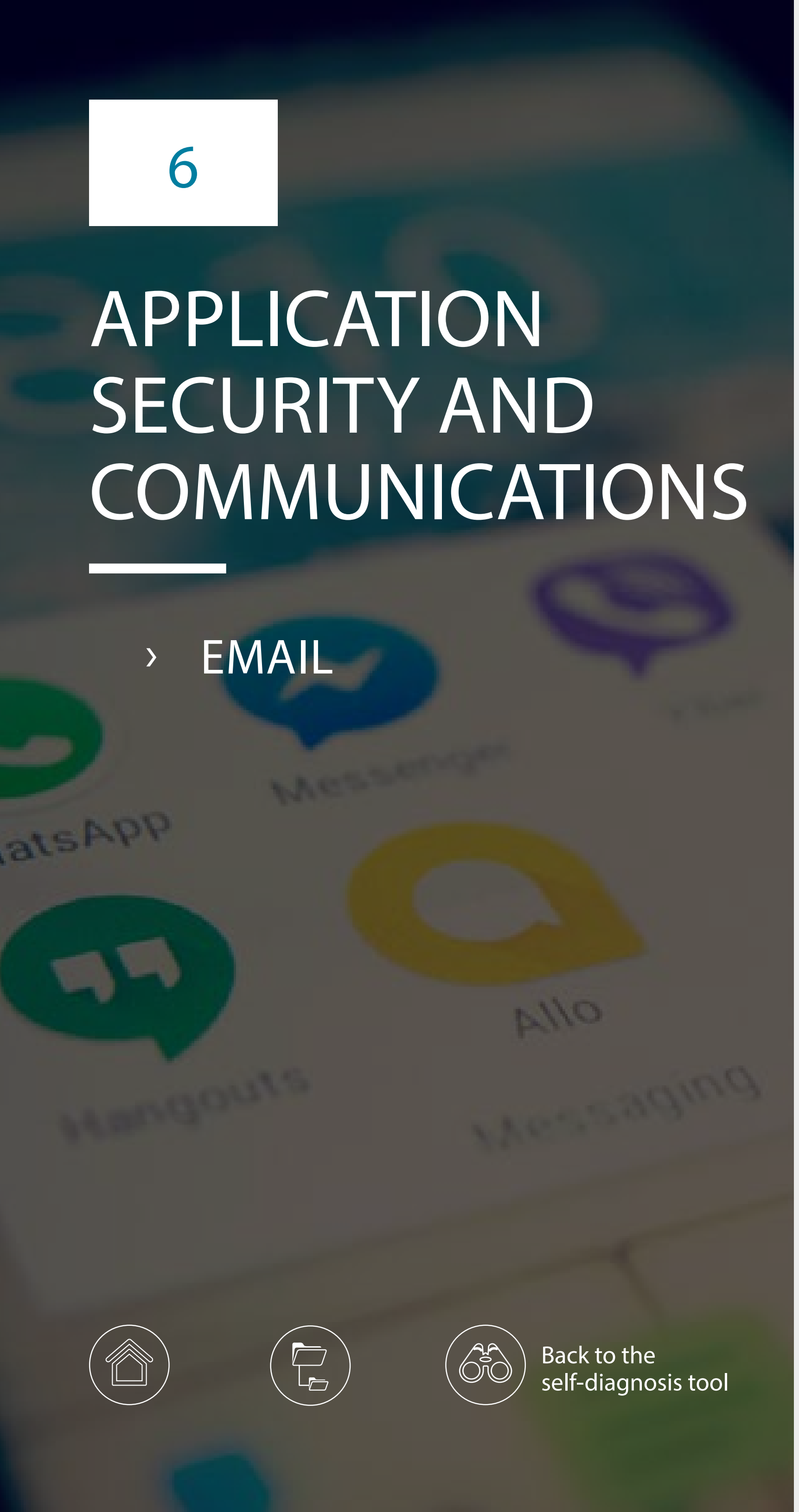
› APPLICATIONS

Back to the self-diagnosis tool

Applications collect, process and communicate data. They often have access to a broad range of information, including contacts, emails, geolocation and documents on the device. Applications are usually found on computers, servers, tablets, telephones and the cloud. Televisions, security cameras, smart watches and other connected devices are also sometimes equipped with applications.

BEST PRACTICES

- Understand how these applications work and what they can access.
- Consider segregating personal and professional data on computers and mobile devices. While this practice makes using the devices more complex (switching between two separate profiles, using different applications), it protects professional data and allows a "freer" use of the device for personal purposes.
- Read the privacy and information security policies (including on confidentiality) as well as the end-user licence agreements (EULAs) of all installed applications, and understand how the data processed by these applications flows.
- Use mobile device applications that store data on the organization's servers instead of on the device itself. If this is not possible, use applications that store data on cloud servers hosted in Canada.
- Regularly update applications.
- Only allow authorized persons to install applications on devices.
- Consider implementing mobile device management solutions.
- Ensure compliance with Canada's Anti-Spam Legislation (CASL).



6

APPLICATION SECURITY AND COMMUNICATIONS

› EMAIL

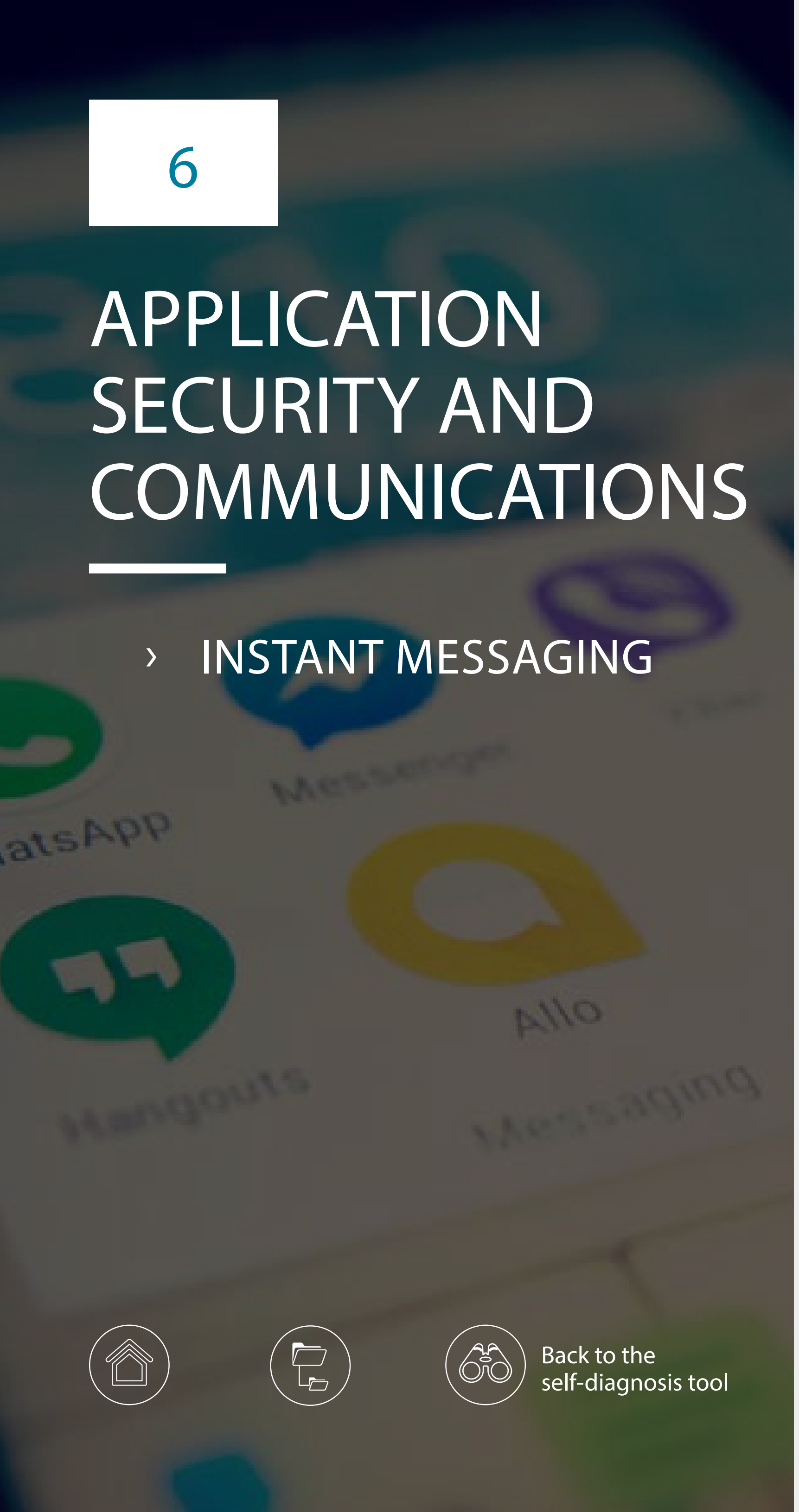
Back to the self-diagnosis tool

When emails are unencrypted, the confidentiality of the information transmitted is not protected.

Email-related risks include the following: interception of unencrypted messages, identity theft, fraud, social engineering (e.g. an email from someone claiming to be the organization's president to a controller of finance to authorize an emergency payment) and cybercrime (ransomware, viruses, malicious logic).

BEST PRACTICES

- Train staff on email scams (phishing, etc.).
- Engage a cybersecurity firm and occasionally conduct social engineering tests.
- Establish third-party authentication procedures before making payments or sharing sensitive information.
- Protect attachments with a password sent through another communication method, or use a secure delivery platform.
- Check the messaging service's terms of use to ensure the service provider does not have the right to use contents for any reason whatsoever.
- Avoid messaging services with servers outside of Canada or that belong to a foreign company.
- Backup email messages.
- Agree on the use of email as a method of communication with clients. Obtain their express consent when sending documents covered by professional secrecy.
- Enable automatic out-of-office replies to notify the sender of absences and the inability to read messages.
- Implement email security solutions (anti-virus, anti-spam, anti-ransomware, etc.) to reduce email related risks.
- Consider implementing mobile device management solutions especially where email, calendar, and contacts data are synchronized to mobile devices.



6

APPLICATION SECURITY AND COMMUNICATIONS

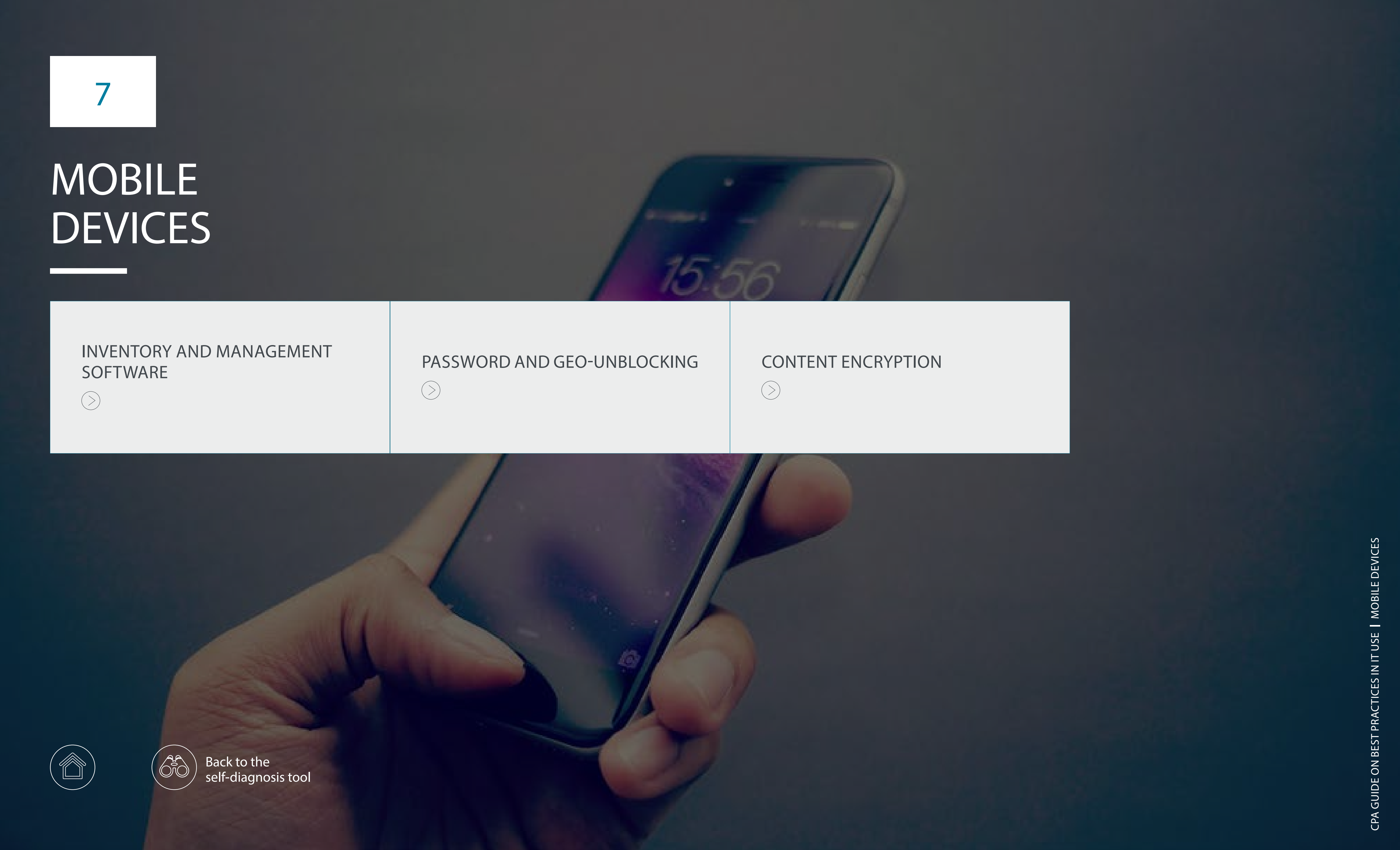
› INSTANT MESSAGING

Back to the self-diagnosis tool

Instant messaging can replace email. If it is only used internally, instant messaging is subject to the same risks as any other application. When instant messaging is also used to communicate with clients, it becomes an additional entry point that needs to be secured. In all cases, there are risks associated with this application, including risks to data encryption (data in transit or at rest), the server location (inside or outside of Canada), and the application publisher's ownership (Canadian or foreign).

BEST PRACTICES

- Understand how the application works.
- Secure the application if it is used to communicate outside the organization's network.
- Check the messaging service's terms of use to ensure the service provider does not have the right to use contents for any reason whatsoever.
- Avoid messaging services with servers outside of Canada or that belong to a foreign company.



7

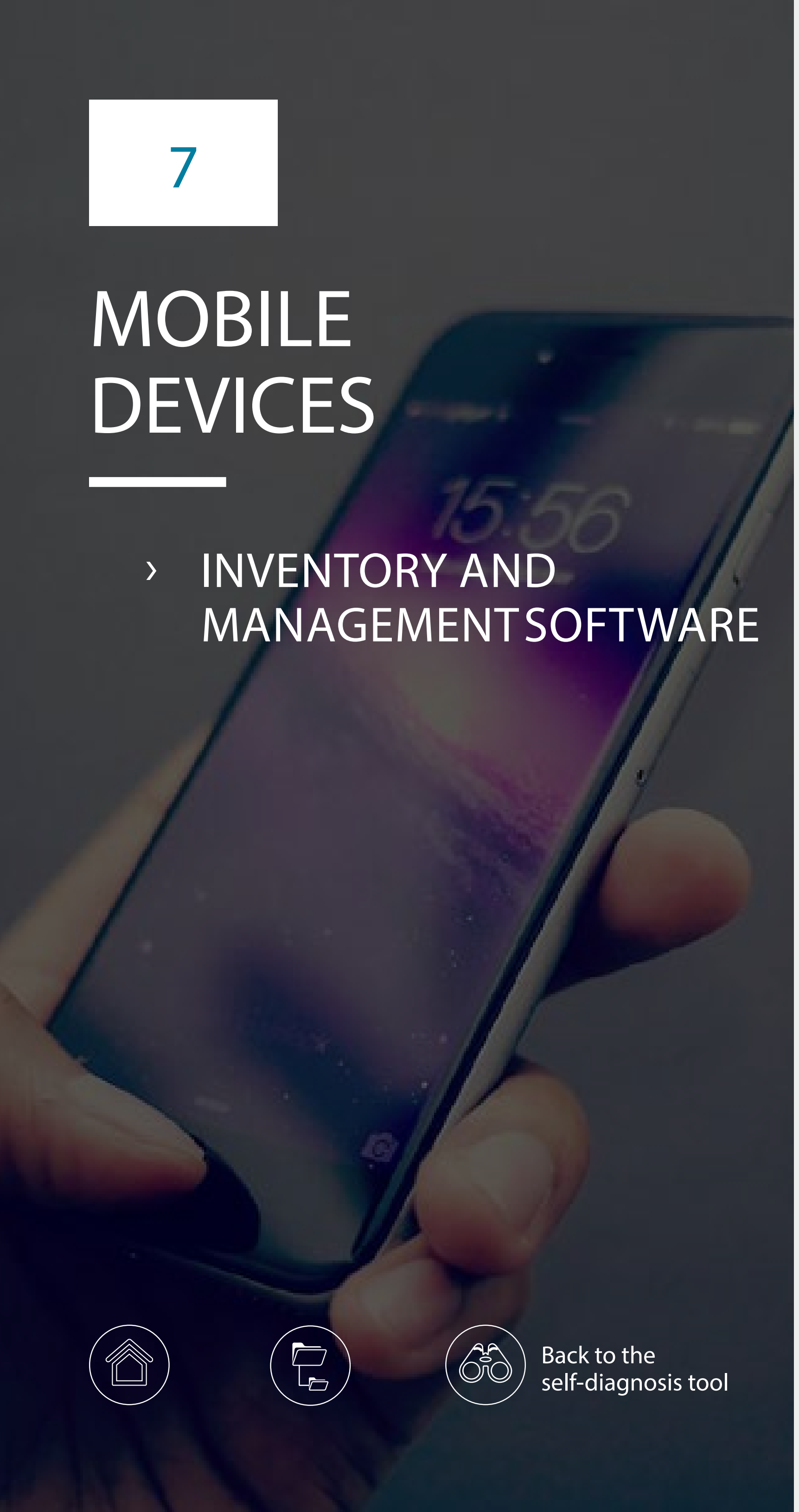
MOBILE DEVICES

INVENTORY AND MANAGEMENT SOFTWARE

PASSWORD AND GEO-UNBLOCKING

CONTENT ENCRYPTION

Back to the self-diagnosis tool



7

MOBILE DEVICES

› INVENTORY AND MANAGEMENT SOFTWARE

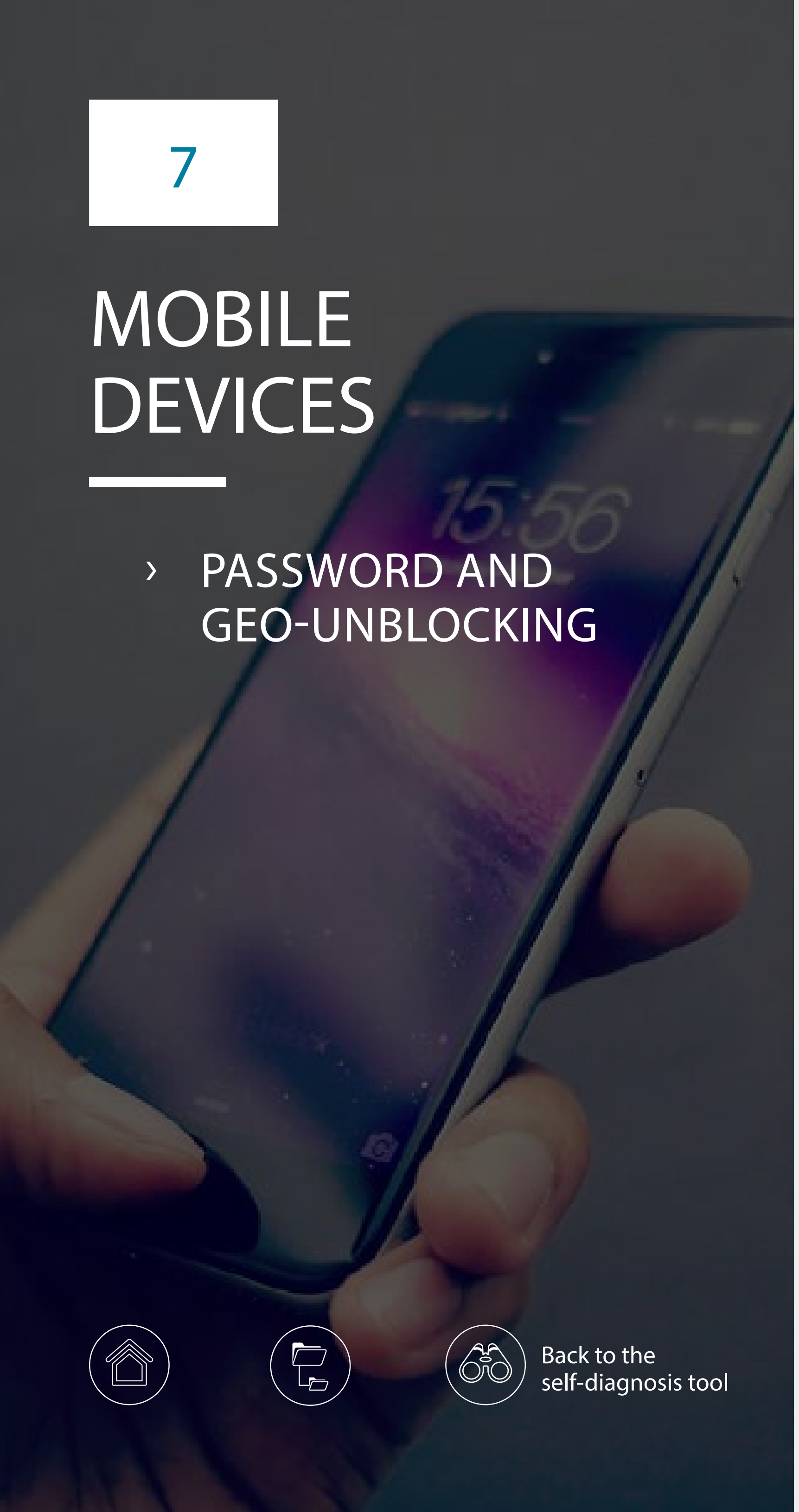
A mobile device inventory should be kept to record losses and thefts, and to manage incidents.

Mobile device management software helps secure mobile devices. It can be used to update applications and operating systems, as well as remotely control devices. This feature is especially useful to destroy data remotely if a mobile device is lost or stolen, or conversely, to save data automatically. If the data on the mobile device is transient (the original data is stored elsewhere or a backup copy exists), there is no risk of permanently destroying data.

BEST PRACTICES

- Purchase mobile device management software.
- In the inventory of issued mobile devices, include the usual identifiers (model, serial number), the versions of the operating system and the mobile device management software, the encryption status, and the device user’s name. Manage the inventory using management software or manually.
- Regularly backup mobile device data.
- Wipe data remotely when necessary.

Back to the self-diagnosis tool



7

MOBILE DEVICES

› PASSWORD AND GEO-UNBLOCKING

Back to the self-diagnosis tool

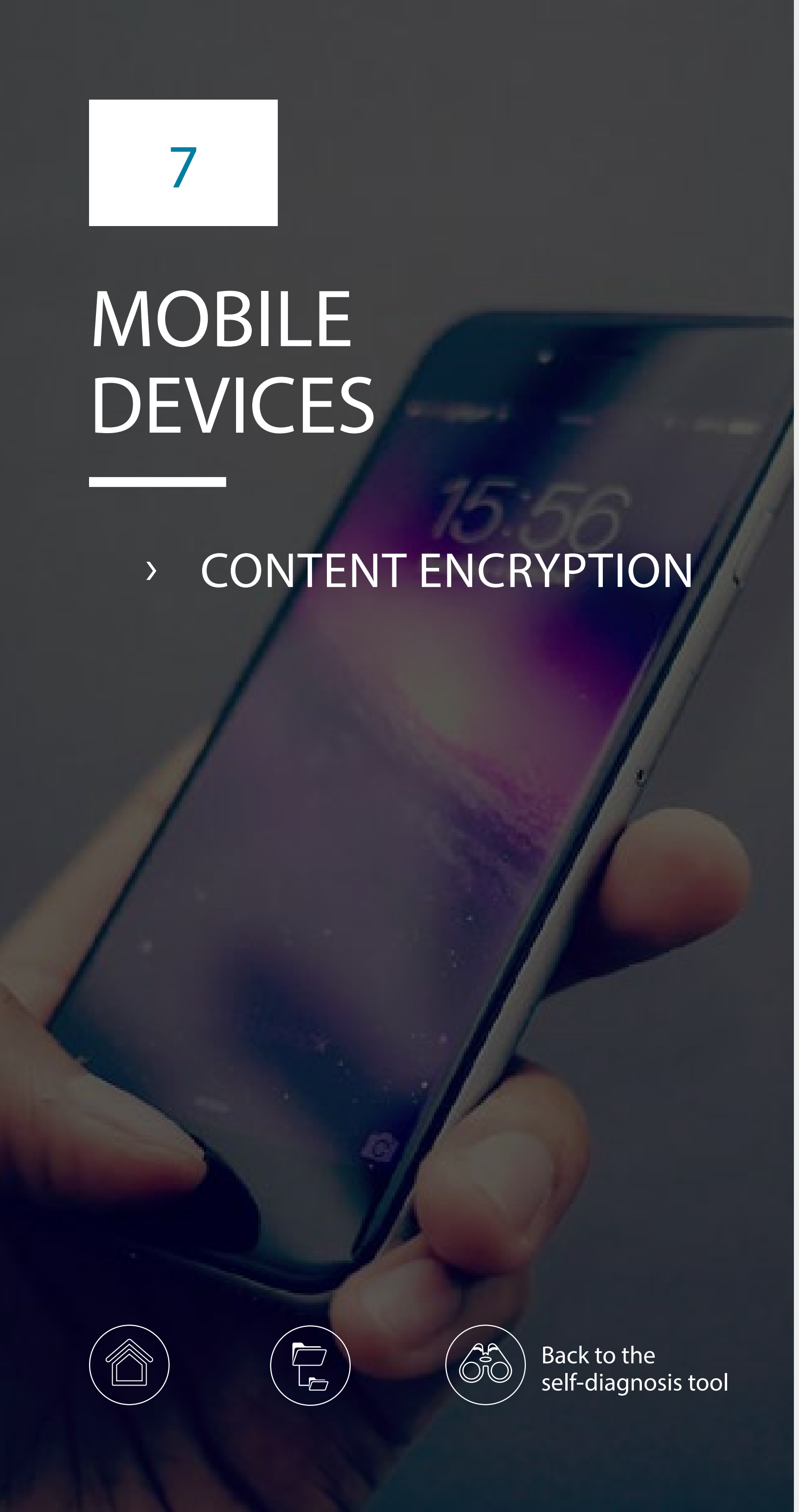
Password requirements for mobile devices are often seen as an irritant. The length and special characters are not adapted to touch screens, and the passwords must be entered often. It is therefore very tempting to automatically unlock devices based on their location (GPS), or when they connect to a specific network. With this practice comes the risk of losing control of devices that would be unlocked automatically when connected to a network, for example, if a device is left in a conference room accessible to the public.

BEST PRACTICES

> Ensure the physical perimeter is secure, that is, do not configure automatic unlock for uncontrolled environments (as opposed to a home or an office that is not accessible to the public).

> Only activate automatic unlock once the password has been entered.

> Configure devices to lock on leaving the controlled environment.



7

MOBILE DEVICES

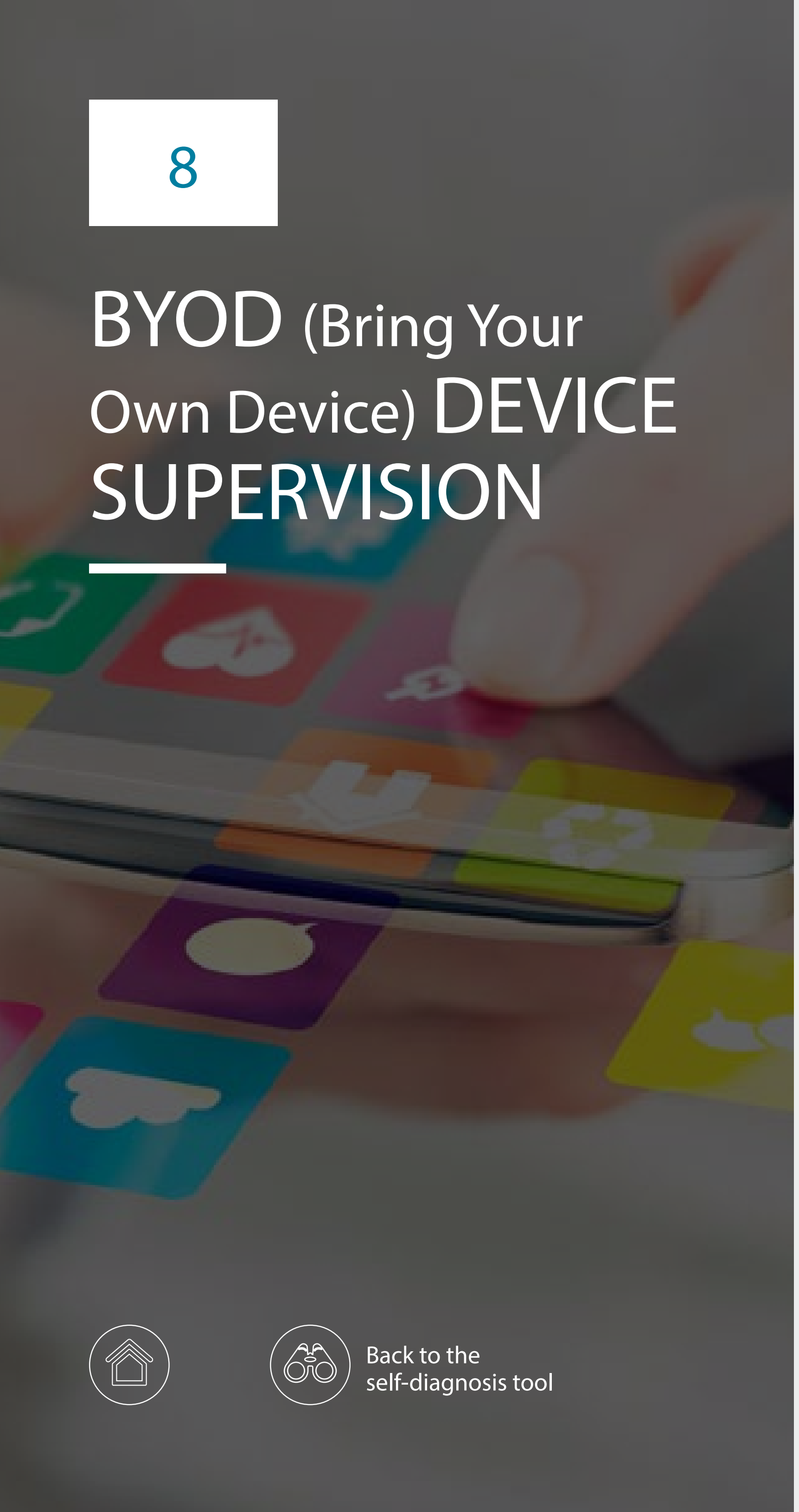
› CONTENT ENCRYPTION

All mobile devices, including laptops, can encrypt content, which can then only be accessed after user authentication. The process is transparent for the user and significantly reduces the risk of a confidentiality breach if the device is lost. Since encryption solutions are very affordable, and even free on certain devices, it would be unwise to do without one. It is also important to protect the decryption key and not lose it.

BEST PRACTICES

- Encrypt the content on mobile devices by activating the function or purchasing the application.
- Secure decryption keys according to how encryption is managed. If encryption is centralized, a software solution can ensure key security. Decryption keys can also be placed in a secure location, like a safe. If encryption is managed by the device and activated by the user with a password, this password must be protected.

Back to the
self-diagnosis tool



8

BYOD (Bring Your Own Device) DEVICE SUPERVISION

Back to the self-diagnosis tool

Many organizations give their employees access to some of their data and applications, including email, via the employees' mobile devices. This has a number of effects on both sides.

The line between employees' personal and professional lives becomes blurred, while employers lose partial control over their data. As such, employees give their employers the ability to access the contents of their devices (phone records, text messaging, etc.) and destroy data remotely. For their part, employers' confidential data flows into a porous environment. To limit these risks, barriers should be placed between personal and professional data.

BEST PRACTICES

> Implement a policy on the use of personal devices in a professional context. This policy should:

- Reinforce the ownership of the organization's information assets.
- Clarify users' expectation of privacy in relation to the employer's right to check how its information resources are being used and to conduct investigations.
- Specify whether mobile device management software will be installed on the devices. The policy should also indicate whether information can be destroyed remotely, if required, in the event of a security incident.
- Require that basic security measures be implemented and kept up to date, including antivirus software.

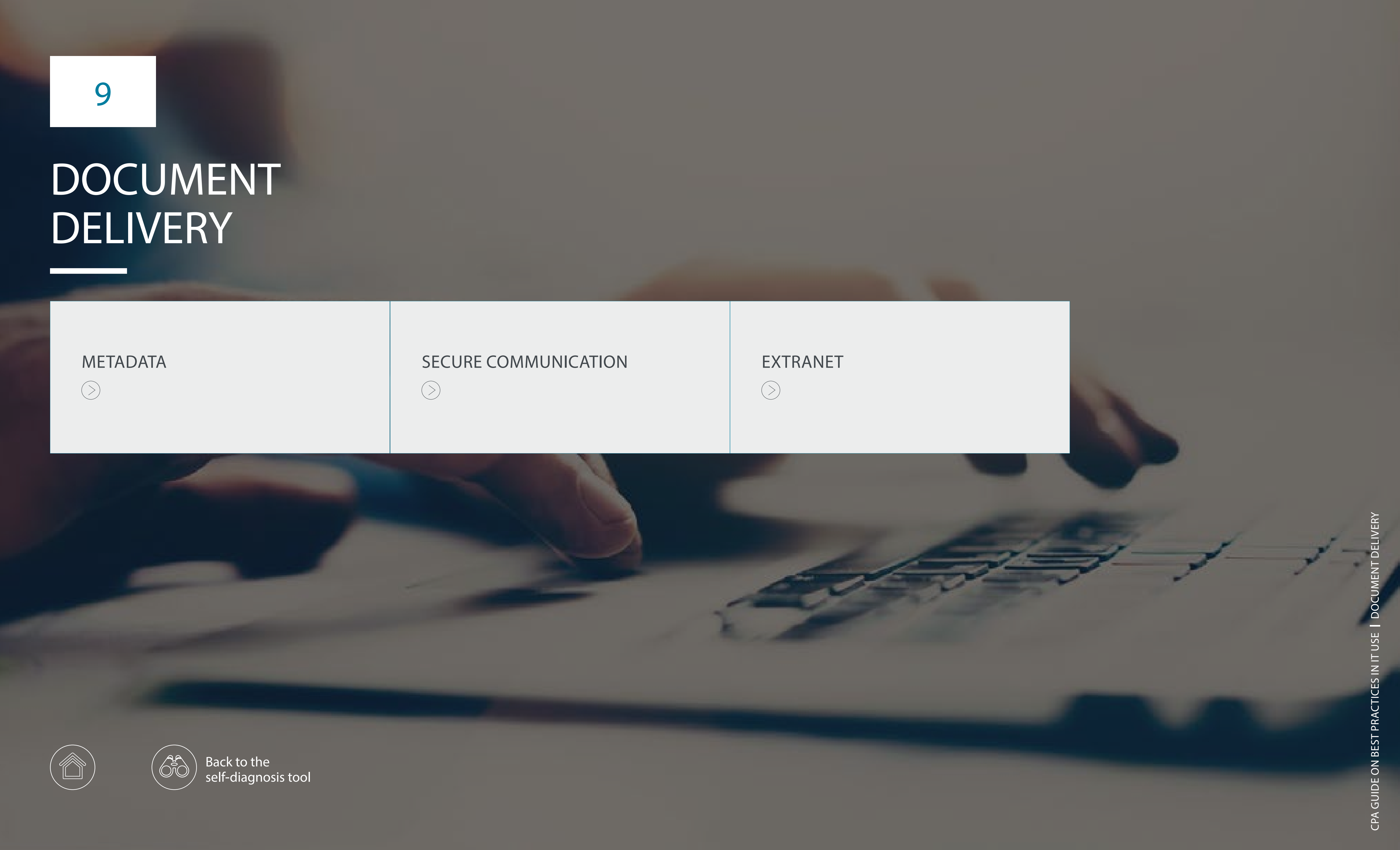
> Consider the loss or theft of a BYOD device as a security incident and set up an emergency telephone number or web portal to report such incidents.

> Inform employees of the policy and ensure their compliance.

> Use segmentation or containerization technologies (usually part of a mobile device management solution) to create the separation between corporate and personal data/applications.

> Limit storage of corporate data on BYOD devices.

> Implement a policy to ensure a copy of corporate data do not exist solely on the BYOD device.



9

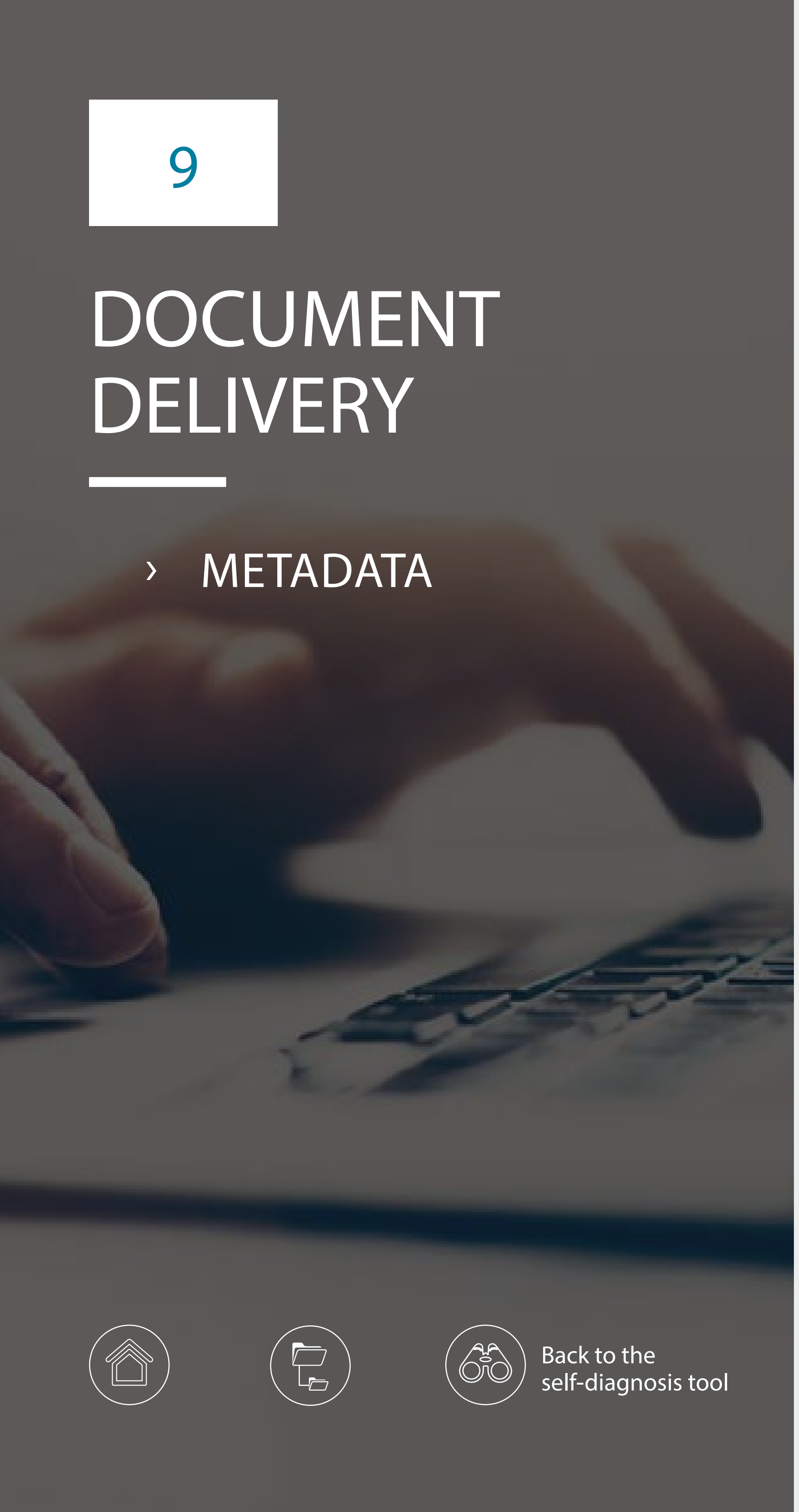
DOCUMENT DELIVERY

METADATA

SECURE COMMUNICATION

EXTRANET

Back to the self-diagnosis tool



9

DOCUMENT DELIVERY

› METADATA

Electronic documents are comprised of data and metadata. Metadata provides information about a document's context, such as creation date, authors, file name, access path in the network architecture, etc. Disclosing some of this information can compromise professional secrecy. For example, professional secrecy can be jeopardized when documents created for one client are used as templates for a subsequent mandate. Most programs make it easy to wipe metadata.

BEST PRACTICE

> Wipe metadata before documents are used or sent to third parties or clients.

Back to the self-diagnosis tool

9

DOCUMENT DELIVERY

› SECURE COMMUNICATION

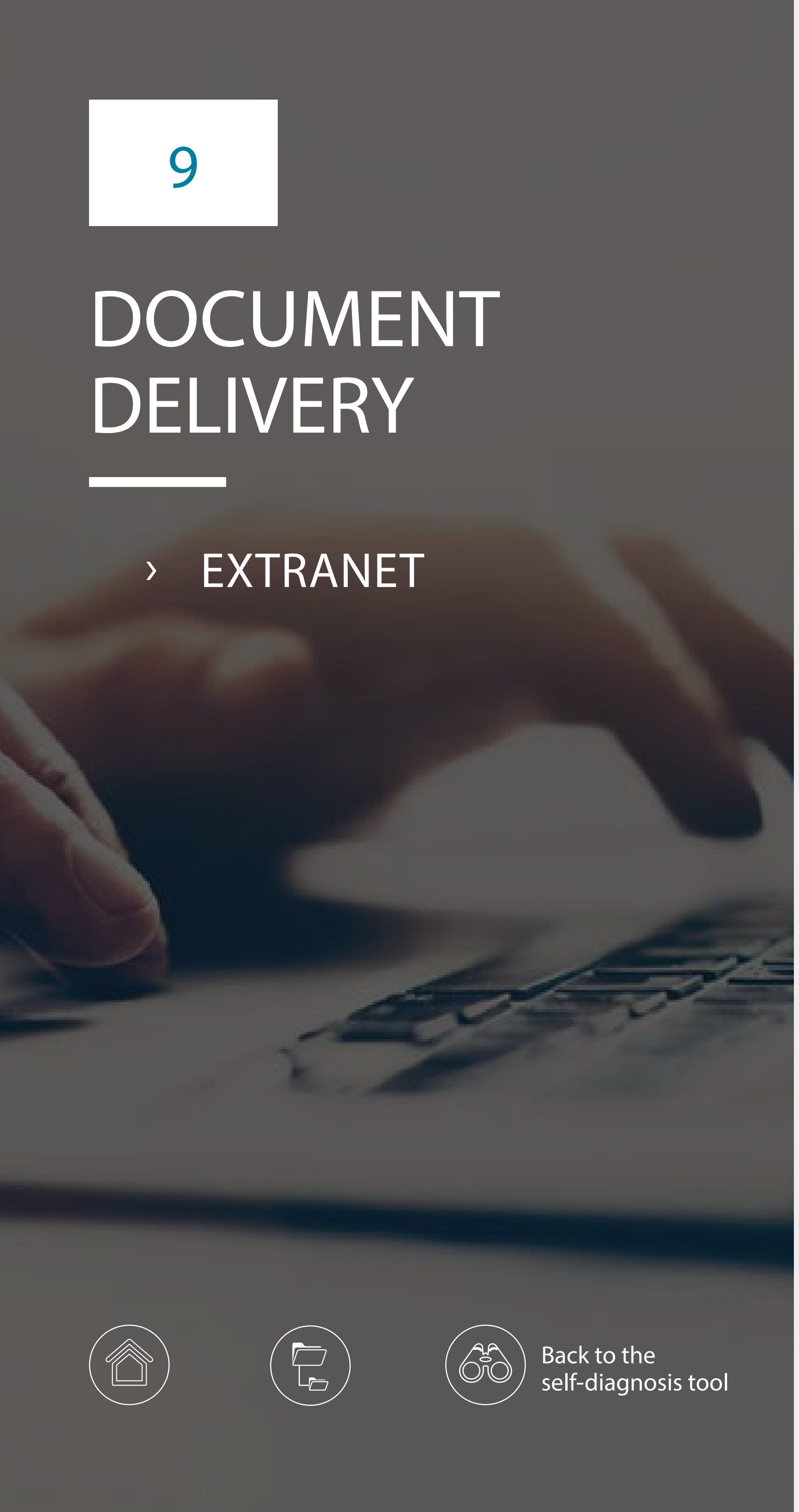
Back to the self-diagnosis tool

Email messages and their attachments are not confidential by default because their contents are unencrypted. This means emails can be read by anyone with access to them, whether legitimate or not, such as a technical intermediary, a free web-based email provider, an intelligence agency, a foreign government or a hacker. A message's contents, including the text and the attachments, can be encrypted. However, a message's headers (date, subject, name and address of the sender and recipients, etc.) cannot be encrypted.

To ensure their exchanges are confidential, CPAs and their clients can agree on a secure communication platform. The sender first uploads a message and its attachment using an encrypted connection. The platform then notifies the recipient, who can retrieve the message and its attachment in the secure environment.

BEST PRACTICES

- Subscribe to a secure communication service for document and message exchange.
- Do not use a free web-based service whose terms of use give the service provider the right to access contents or use them for any reason. Also, avoid using a service with servers located outside of Canada, or a service whose provider is a foreign company.
- In the engagement letter, provide for security measures to be put in place to protect the confidentiality of exchanges. This can include a choice of platform for document sharing.



9

DOCUMENT DELIVERY

› EXTRANET

Back to the self-diagnosis tool

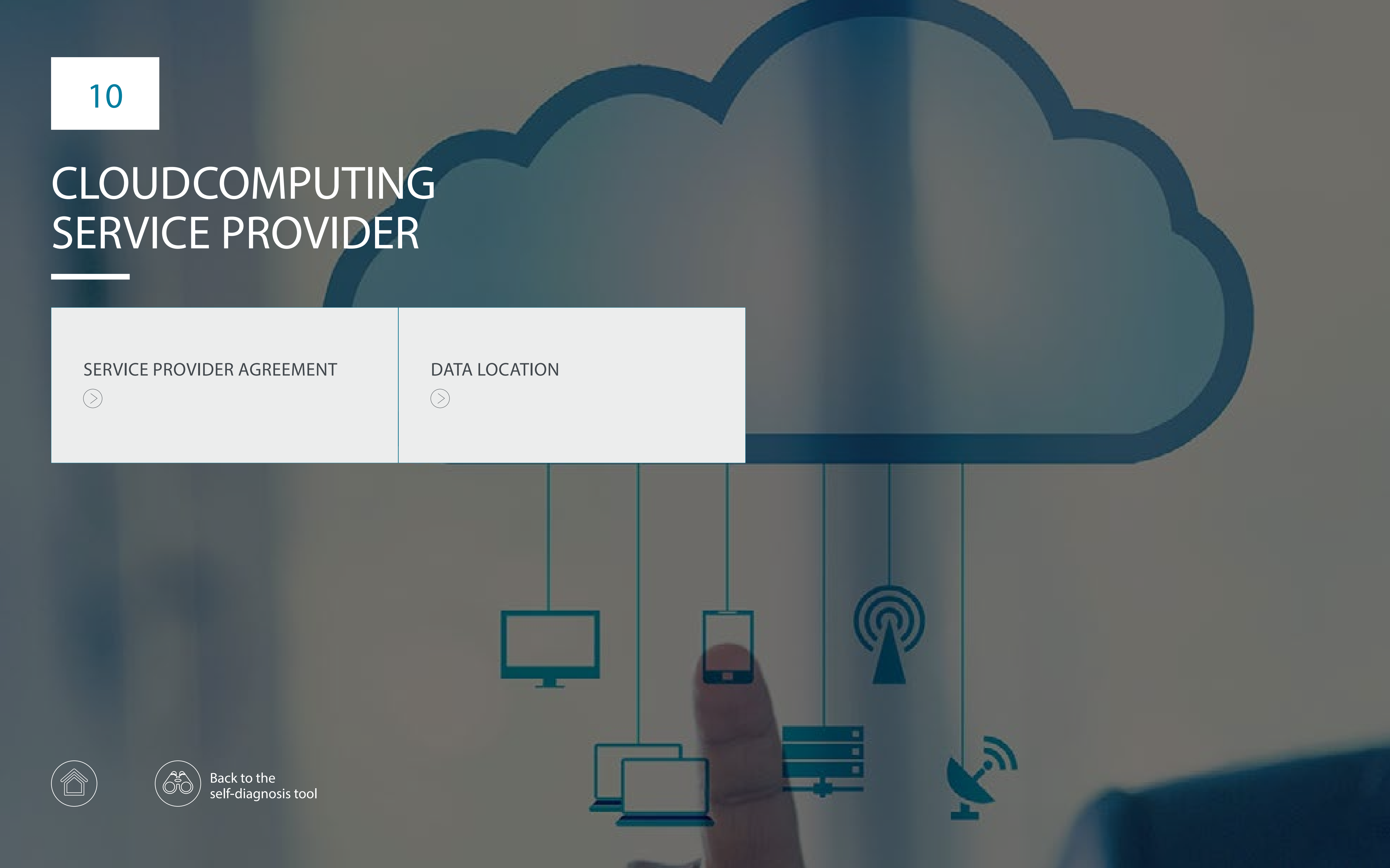
Organizations can host their own secure platform to exchange documents and share access to their information resources. For example, they can make applications available to their clients to conduct simulations. Privacy risks are thus managed more effectively. However, opening up the internal network to outsiders may affect document retention security.

BEST PRACTICES

- Implement appropriate security measures, including application updates, two-factor authentication, and network segregation to isolate certain elements (applications, client data and organization data).
- Conduct a penetration test.

10

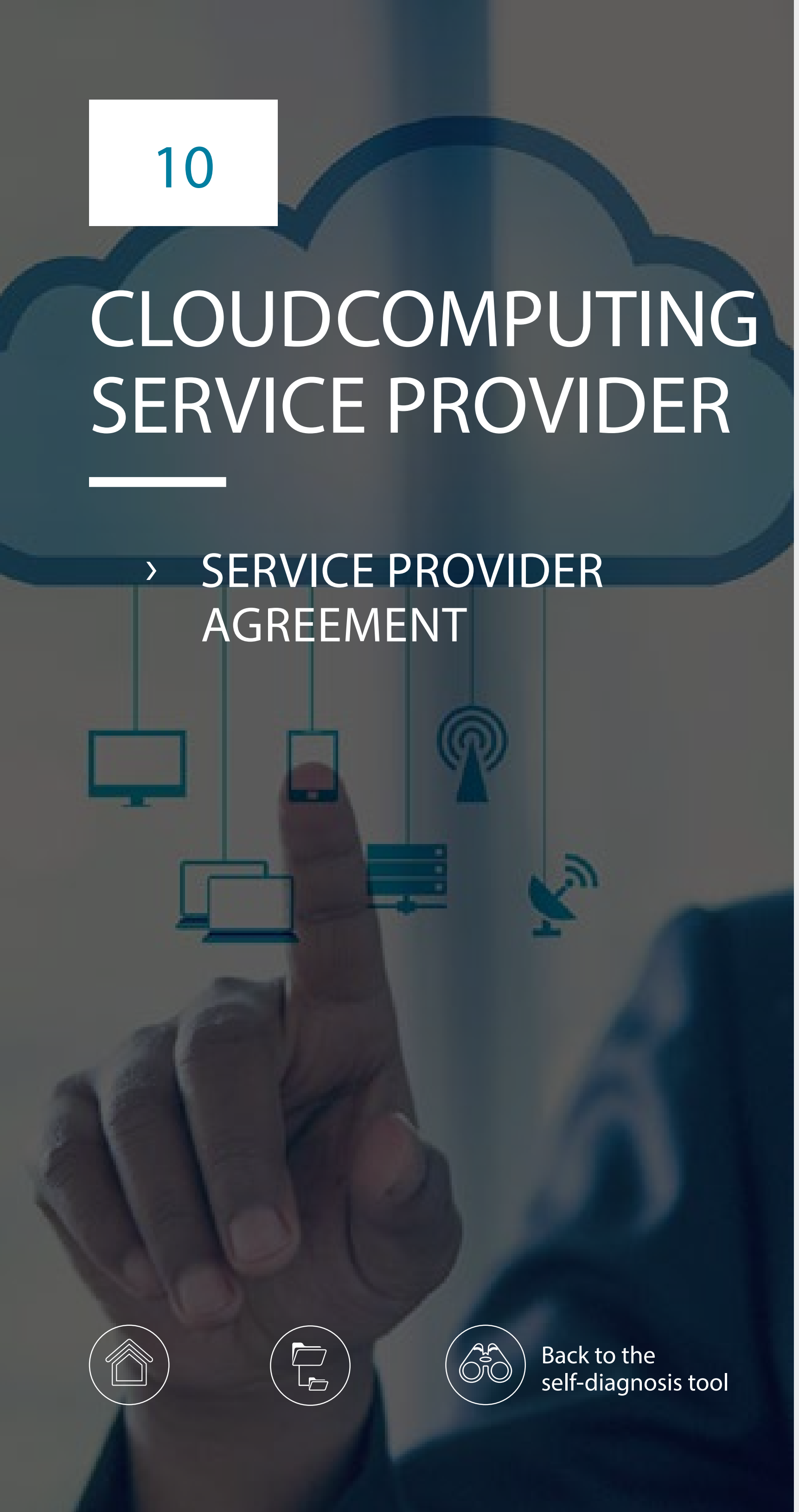
CLOUDCOMPUTING SERVICE PROVIDER



SERVICE PROVIDER AGREEMENT

DATA LOCATION

Back to the self-diagnosis tool



10

CLOUDCOMPUTING SERVICE PROVIDER

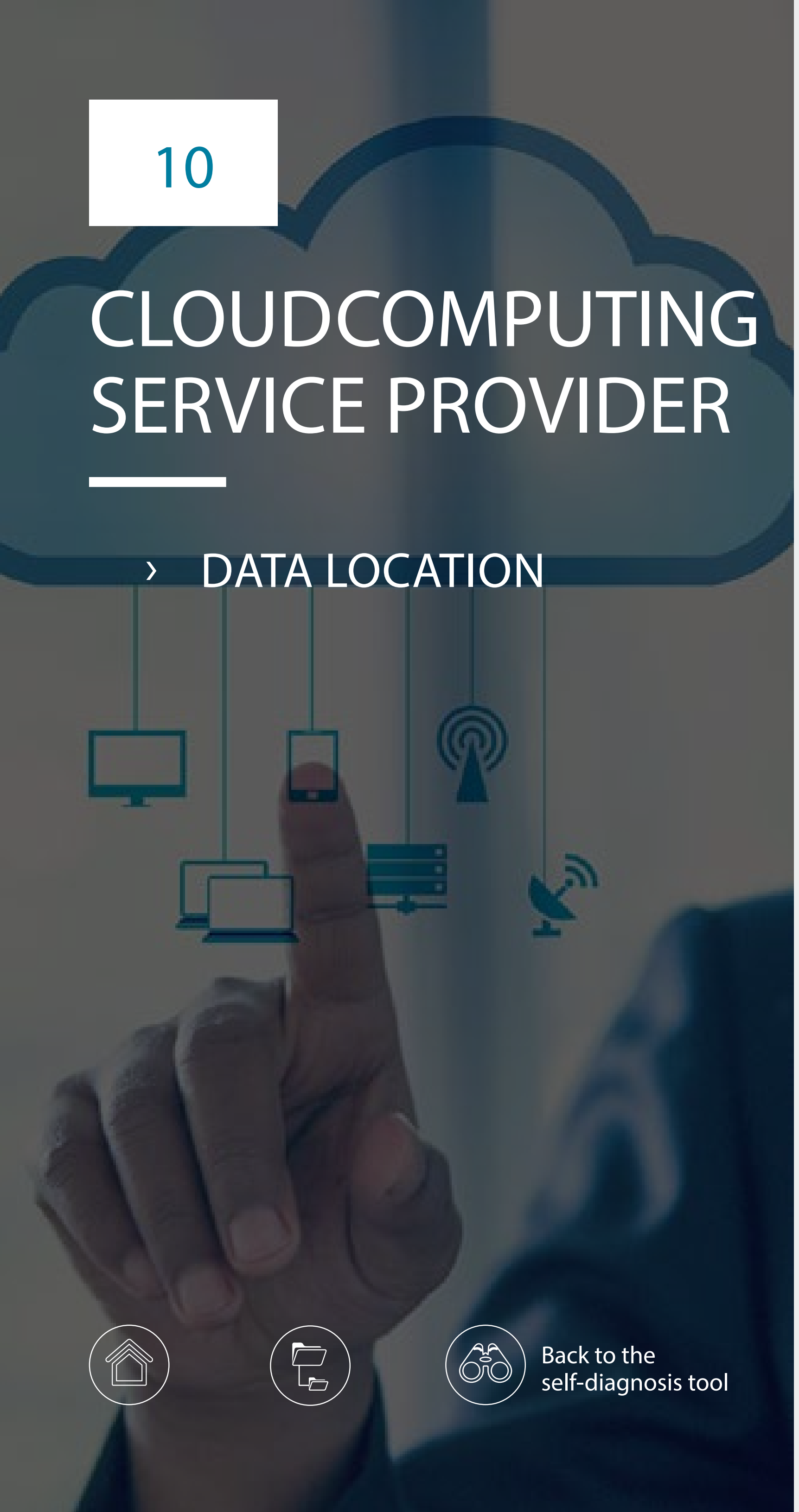
› SERVICE PROVIDER AGREEMENT

Back to the self-diagnosis tool

The term cloud computing includes everything related to offsite computing. In other words, it refers to computer resources (data hosting, software, platforms) managed by a third party to varying degrees. Cloud computing has clear cost benefits and potential information security advantages, depending on the partner's maturity. Still, the service agreement must contain specific provisions regarding information security and professional secrecy.

BEST PRACTICES

- Consult a cloud computing specialist to better understand the proposed agreement and ensure security requirements are clearly specified.
- Include provisions in the contract governing the end of the agreement with the cloud computing service provider which cover the following:
  - Data ownership
  - Notices
  - Data retrieval and format
  - Mandatory notification in the event of a confidentiality breach or data theft
  - Possible audit
  - Use of third-party services
  - Access to data and migration should data be destroyed or the services terminated
- Consider data loss insurance.
- Inform clients that data is stored on an external server.
- For BC, FOIPPA applies to storage and access of PII (personally identifiable information). This should be stipulated in the contract with the service provider.



10

CLOUDCOMPUTING SERVICE PROVIDER

› DATA LOCATION

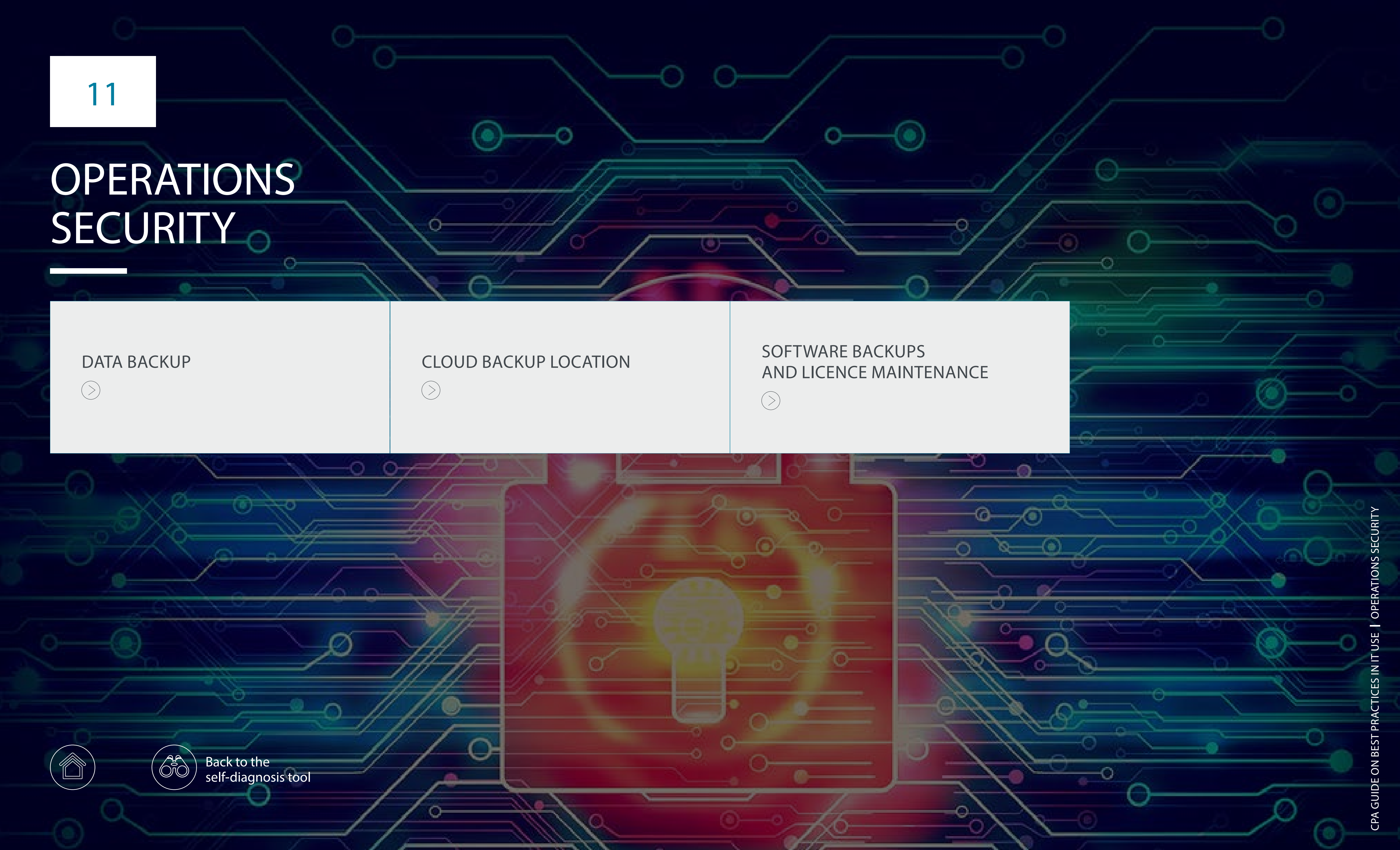
When data is on a provider's network, the data's location is unknown to the user. The location of the data can change quickly based on the availability of the resources of the provider, who may also be doing business with other service providers. If a foreign provider is involved, the data may be subject to foreign laws.

Certain clouds are restricted to specific geographic locations, which means the data flows within established borders (e.g. Canadian cloud); this reduces the risk of losing control over data location.

BEST PRACTICES

- Avoid free cloud services, clouds without a location or clouds located outside of Canada. Also, avoid foreign providers.
- Inform clients of the risks and obtain their consent to use certain technologies.
- For BC, FOIPPA applies to storage and access of PII (personally identifiable information).

Back to the self-diagnosis tool



11

OPERATIONS SECURITY

Back to the self-diagnosis tool

11

OPERATIONS SECURITY

› DATA BACKUP

Back to the self-diagnosis tool

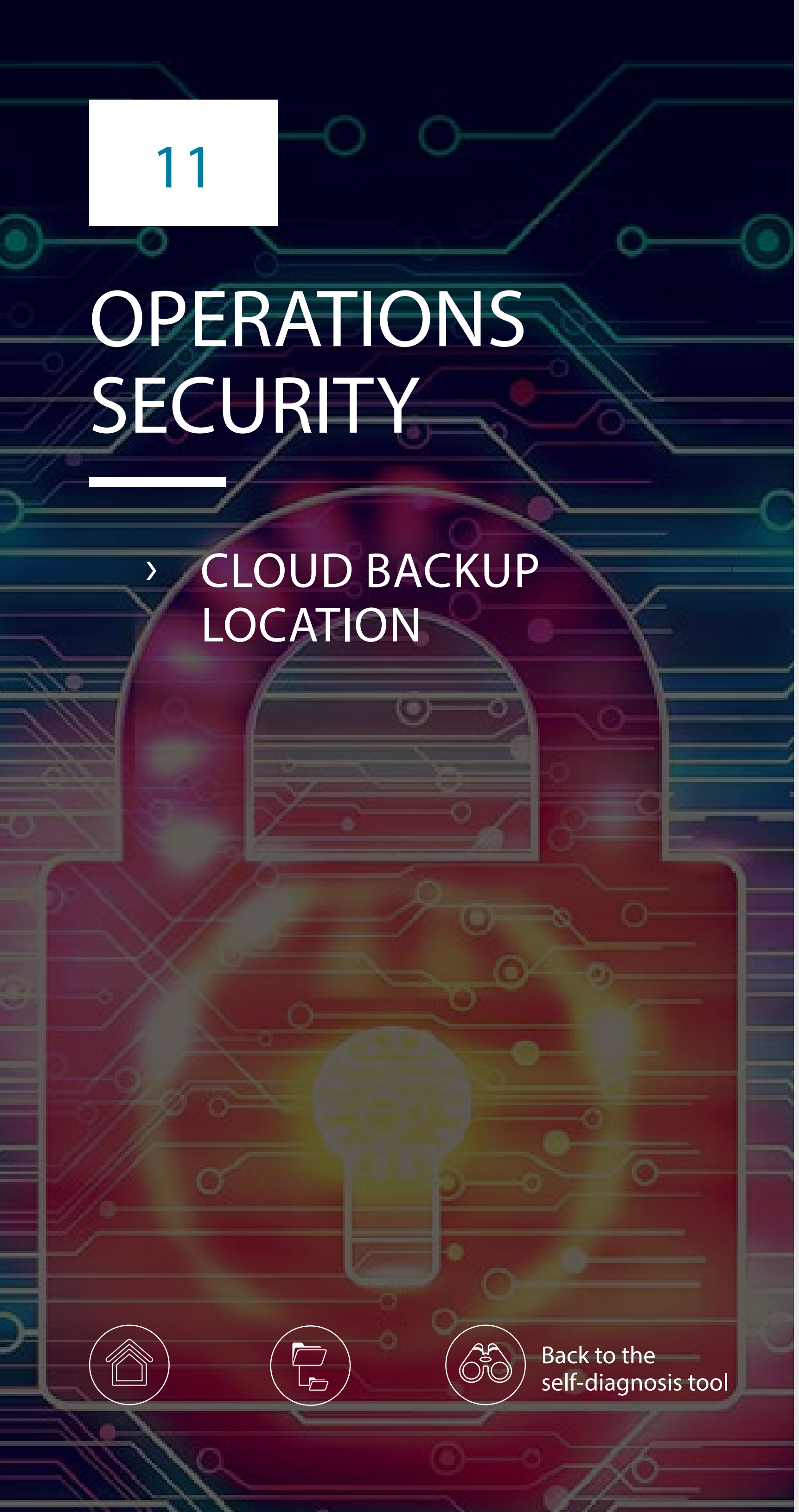
Backup copies ensure that data remains available in the event of a disaster. They mitigate the risk of data corruption (virus, geomagnetic storm, computer bug, etc.) or the loss of all master data (through theft, ransomware, etc.). Creating backup and archive copies requires two different processes.

Software packages offer various backup modes. The most common involves performing a full backup periodically, and then incremental backups including only information that has been changed or added since the last full backup, which requires less time and storage.

Backup copies should also be encrypted. As the last resort to retrieve data, they should be accessible and highly reliable. Securing the decryption key is crucial.

BEST PRACTICES

- Implement a backup schedule.
- Use a combination of full and incremental backups.
- Perform a full backup before changing providers or terminating an agreement.
- Implement a backup retention scheme.
- Keep previous backups until they are replaced by a new complete copy.
- When backups are stored on physical media:
  - Encrypt the media's content.
  - Place the decryption key in a secure location ~~like a safe~~.
  - Store encryption and decryption passwords in a password manager.
- If data is backed up to a service provider's server, the connection should be secure and the data encrypted. Encryption is not necessary if the provider's security measures ensure sufficient protection (for example, confirmed by an expert report).
- Periodically conduct data retrieval tests.
- Include provisions in the cloud service provider contract on data retrieval, if needed, and testing.
- Verify integrity of backup recovery points.
- Give preference to local providers that can quickly and safely deliver backups on physical media.
- Destroy data in accordance with retention policies.



11

OPERATIONS SECURITY

› CLOUD BACKUP LOCATION

Back to the self-diagnosis tool

Since the backup must be useable if all of the master data is lost, it should be physically separated from the master data. If a risk event occurs that affects the master data, the backup should not be impacted. Therefore, backups should be stored in a separate location, such as in a safe in another building.

Similarly, the backup must be logically separated, to prevent corruption of the master data by malicious software (e.g. ransomware). Therefore, the medium must not be connected to the computer system once the copy has been made. The medium used should be reliable and able to resist environmental factors (heat, humidity, shocks, friction, static electricity, etc.). The amount of information to backup will determine the choice of medium. For example, an external hard drive can be used for full backups and optical disks for partial backups.

For cloud-based backups, hard drives and optical disks will not be required. Instead, it may directly synchronize from the source to the cloud-based backup "target". The source can create a backup to a local appliance (local cache) which in turn gets synchronized to a cloud-based target.

When data is backed up to a remote server belonging to a service provider, the required measures are the same as for a cloud-based service.

BEST PRACTICES

- Keep backups in secure locations separate from where the master data is hosted.
- Disconnect external hard drives as soon as the backup is complete.
- Treat backups like any other cloud service. Perform the same checks and validate the data retrieval method.
- Avoid free cloud services, clouds without a location or clouds located outside of Canada. Also, avoid foreign providers.
- Choose reliable data media based on their resistance to unfavourable environmental factors and the amount of information to be stored.
- Avoid using USB sticks to save data, as they are easy to lose.

11

OPERATIONS SECURITY

› SOFTWARE BACKUPS AND LICENCE MAINTENANCE

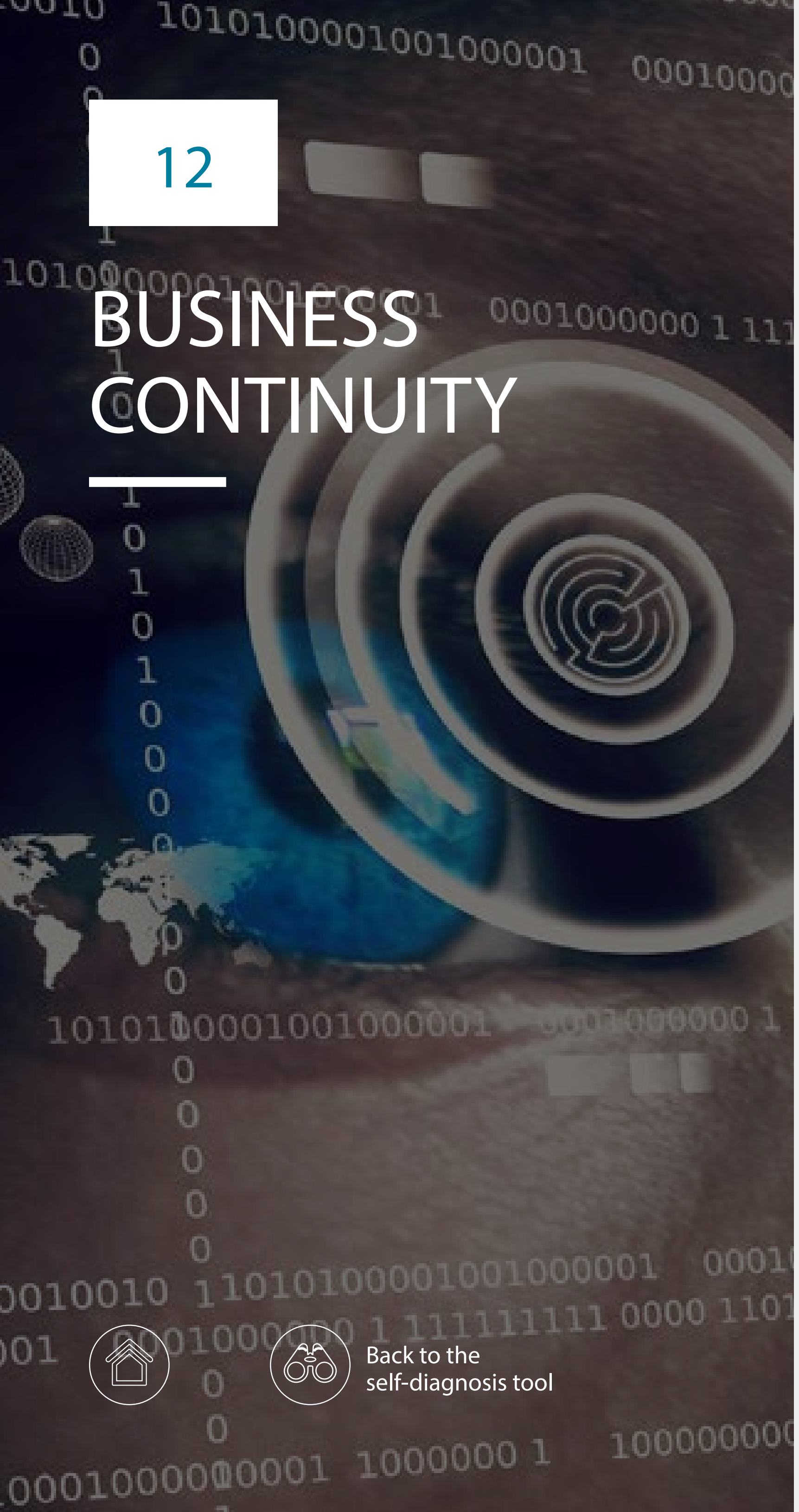
Back to the self-diagnosis tool

Maintaining software capability involves backing up software and configuring the more complex programs.

In addition, the right to use software tools under licence agreements should be maintained over time.

BEST PRACTICES

- Backup the computer system's software (physical medium or downloaded installer file).
- Inventory the software and establish a licence management process to detect when the number of licences is insufficient for the software's usage (e.g. too many users, too many users at the same time, installation on too many devices).
- Make sure the licences of software in use are in effect, in particular specialized software, to preserve access to the data.
- Consider migrating files to a more permanent format, for client file retention purposes.



12

BUSINESS CONTINUITY

The resilience of any organization, large or small, depends on its ability to continue operating no matter the type of disruption it faces. This is especially true for professionals such as CPAs, who often have to work under deadlines and keep records of their activities for a period of time after the end of their mandates.

In order for CPAs to continue their activities and meet their ethical obligations, they should implement several measures. These measures include a business continuity plan and a procedural guide that explains what to do if a major disruption affects the organization (catastrophe, accident, epidemic, supply chain issue, sudden closure of a cloud computing service provider, etc.).

An organization's business continuity plan must also take into account disruptions that could affect information resources. Lack of preparation to address these disruptions could slow down the resumption of normal operations, resulting in an ethical breach if services are not rendered on time. It is important to note that the force majeure exemption, where relevant, only applies for the duration of the impediment.

BEST PRACTICE

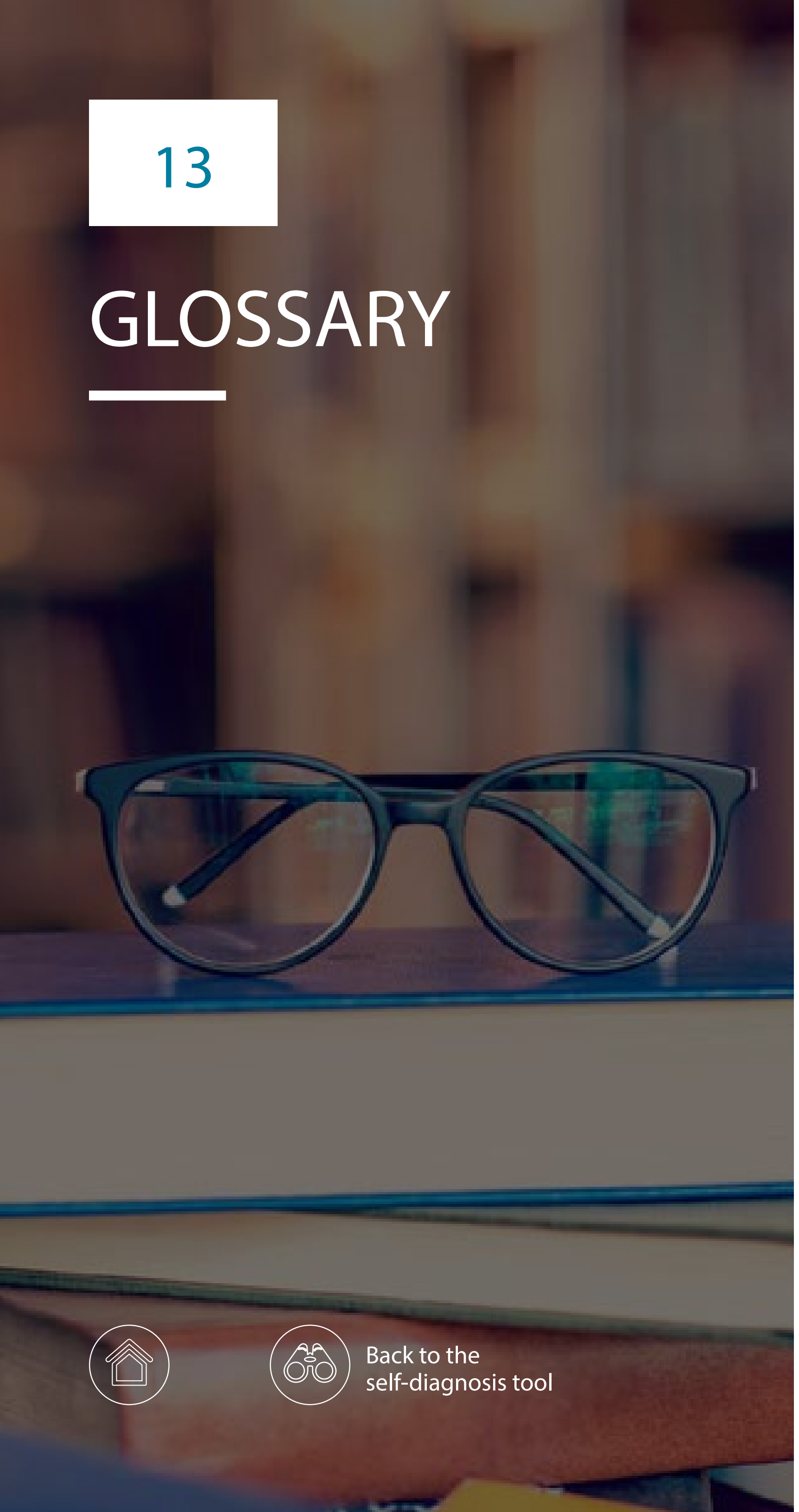
> Develop a business continuity plan that includes the following:

- A prevention component with a backup plan.
- A plan to be carried out simultaneously in the event of a disaster, including staff deployment, disaster recovery and return to normal.
- A plan to manage the incident that caused the interruption of operations.
- A communication plan.
- A recurring test plan to validate operations.
- Establish recovery point objective (RPO) and recovery time objective (RTO) targets.

Back to the
self-diagnosis tool

13

GLOSSARY



Back to the self-diagnosis tool

Term	Definition
BYOD	Bring Your Own Device, a practice where employers allow or require employees to use their own electronic equipment for work purposes.
Encryption key	Key that encrypts data and makes it unreadable to anyone who does not have the decryption key.
Geoblocking, geo-unblocking	Practice that limits access to online resources based on the user’s geographic location.
Hash value	Number generated by a hash function, which is a calculation that creates a digital fingerprint by converting a message of arbitrary size into a code of fixed size for authentication or storage purposes.
Identifier	User name and password that validate a user’s identity in a system.
Information asset	The information itself, regardless of medium (paper or electronic), as well as the systems used to process, use, store and share the information internally and externally.
Logical access	Access to an information system controlled by an identification, authentication and authorization protocol.
USB stick	Small, removable medium or mini hard disk in the form of a key or keychain enabling data to be stored and transferred from one computer to another by inserting the key into the USB ports.
Physical access	Access to a location, building, room, hardware infrastructures (e.g. server room) or specific equipment (e.g. a safe).
Service level agreement (SLA)	Written agreement between a service provider and a client, which defines the levels of each service provided. SLAs generally cover hours of service, availability of service, customer support, production levels, information about the expected security, costs and terminology.
Social engineering	Relies on interactions between individuals through trickery to extort information that will be used to fraudulently penetrate a system or otherwise defraud an organization.
Virtual private network	Network established by creating permanent specialized links between internal networks through public networks, to meet users’ resource sharing needs.