

LAWYER INFORMATION SECURITY BASIC GUIDELINES

Thando Toto
Diogo Duarte
Nicolas Torrent

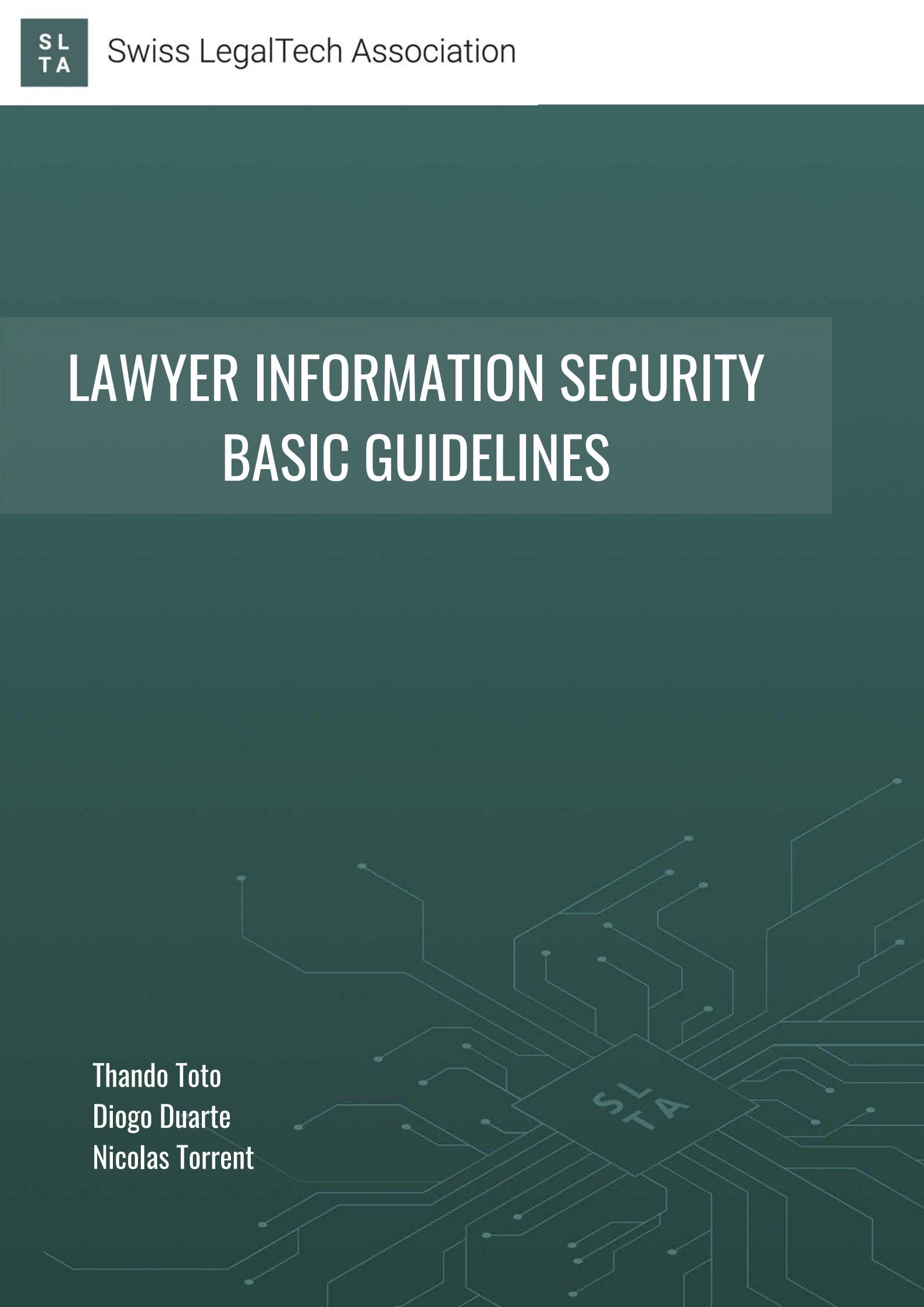


TABLE OF CONTENTS

3

INTRODUCTION

4

MAIN THREATS

5

RISK ANALYSIS

6

BASIC PROTECTION

12

USEFUL TOOLS

14

DISCLAIMER

INTRODUCTION

Law firms are currently being attacked for information about specific targets among their clients but also to collect data with the hope that it will become useful in the future. Indeed, law firms are perceived as a source of valuable financial, corporate and personal information, as well as trade secrets, mergers and acquisitions data, intellectual property, and more.

Even if a law firm is not an identified target, it may still be hacked for the purpose of using it as a "launching pad" to attack other targets, for example by sending counterfeit emails or requesting sensitive information.

Cybercriminals intend to profit from law firm credibility to trick victims. Law firms may also be unintended victims of a sweeping attack to exploit a given vulnerability in a given software.

Cybercriminals fully understand that stolen client data can, in particular, unlock online banking accounts, allow fraudulent money transfers or impersonations. They know how to use the information gathered to engage in further unlawful activities, while the law firms may have to defend against allegations of criminal activity against them.

Every organization can and will be hacked. However, analyzing the risks a firm faces and having the appropriate security measures in place can significantly mitigate the risks and, in the event of an intrusion, mitigate - if not avoid - the damage.

If your stolen data was encrypted, the damage may be insignificant because the data would be unreadable. There would be a need to investigate the exploited vulnerability in the firm's software and secure it; but this is a preferable outcome.

As law professionals progressively adopt new technologies and increase their online presence, they increase the risk to their data if they do not implement, in parallel, the required security.

Performing a risk analysis to identify potential threats and implementing the appropriate measures will help to mitigate the risk of a successful attack and any damage done.

This guide was elaborated to provide a "getting started" guide, on the basis of our common goal and dedication to improve security practices and raise awareness. Quick and easy improvements could be made to the legal industry's information security practices and we decided to contribute with this dedicated guide.



1. MAIN THREATS

Insiders

Insiders include partners, associates, employees, consultants, cleaning staff, third-party service providers and anyone who has some level of authorized access to your firm's internal network or its premises. These insiders may cause a security incident if they engage, intentionally or not, in unsafe practices.

Example: using the same password for all devices and social media account. If a password is compromised, it can be used to access all accounts controlled by that user, including your law firm's network. Likewise, insiders often cause a security incident by failing to recognize a phishing email. According to a PhishMe research*, 91% of attacks succeed because users fail to recognize these emails and click on malicious links, thus unlocking your firm's network to attackers.

These threats are mitigated by a simple information security policy, designed by an Information Security Expert (see p. 6).

*<https://phishme.com/2016-enterprise-phishing-susceptibility-report>

Hackers

Hackers come in many forms and they can have either a malicious or a virtuous intent. This brochure focuses on hackers with malicious intent - also known as BlackHat hackers (as opposed to WhiteHats). BlackHats sometimes operate on their own for online fame or financial gain. They can also be part of organized crime.

Common reasons to intentionally target and hack into a specific law firm include client data theft, damaging the firm's image, gaining information about a competitor and its clients or damaging that competitor or the lawyers representing the client themselves.

It is however more likely that your firm will be an unintentional target: hackers often automatically scan a large number of IP Addresses* in search for a specific vulnerability. Any device affected by this vulnerability will be hacked.

Discuss with your Information Security Expert and your IT specialist to assess the exposure of your firm's network.

* the address of a device on the internet. Example: 26.51.213.107





2. RISK ANALYSIS

What keeps you awake at night?

The first step towards improving information security is to perform a risk analysis. This helps identifying and understanding your risks and applying the appropriate security measures to mitigate these risks.

The best way to perform an information security audit is to mandate an expert in information security, who should ideally be a certified ISO 27001 auditor. This expert will be able to ask you the correct questions and guide you to the level of security that is adequate for your law firm, consistent with your budget, and make the technical, organizational and access control recommendations that will allow you to reach the desired level of security.

In this brochure, we will refer to this expert as your Information Security Expert.

3. BASIC PROTECTION

Data backups

Back up your law firm's data regularly. Regular backups of your data can prove very effective in protecting your law firm against ransomware.

1) Identify the data that needs protection and organize it logically to make it easy to find and retrieve from your backup storage.

2) Ask your IT specialist, in coordination with your Information Security Expert, to choose a storage that has no permanent connection to your network to prevent ransomware from finding the location of your backups and encrypting them.

Options for backups include USB drives, portable drives or an appropriately certified cloud storage provider.

Access to the backups should be restricted and limited to as few individuals as possible.





Malware protection

Malware, short for “malicious software”, is essentially designed to disrupt, damage, or gain unauthorized access to, your network, computers or data. This list provides basic protection against malware. If you are unsure on how to enforce this list, share it with your IT specialist.

- All your computers must have anti-virus software installed and automatically updated.
 - Staff user accounts should only have the rights necessary to perform the tasks pertaining to their job description.
 - Regular users should have regular accounts - not administrator accounts.
 - Enable automatic updates of all software where possible and regularly ensure that your software is up-to-date.
 - Removable media (such as USB sticks) should not be used to share data, as they can contain malicious code or software. Use instead a shared folder on your network, your cloud storage or your collaborative software as a means to share files.
- Enable a firewall to protect your network from intrusion. Firewalls block access from unwanted sources into your network, drastically reducing the load on your computer's anti-virus and anti-malware programs. You should configure your firewall in cooperation with your IT Specialist and your Information Security Expert.
 - In the event of a suspected unlawful activity, have a reporting process to your IT Specialist and your Information Security Expert. If you suspect a ransomware, immediately disconnect your computer from your network and immediately notify your IT Specialist and your Information Security Expert. With your smartphone, take a picture of any message that appears on your screen and share it with your IT Specialist and Information Security Expert.

Password & computer access protection

The most secure way to protect passwords is with a password manager (see p. 13). Its purpose is to create complex passwords and store them securely, without you having to remember any.

Simply create passwords when you need them and record them in your password manager, which should be available on your desktop computer and smartphone - if you use one.

In addition, the following principles should be followed:

- Ensure that all computers are encrypted to protect your data in case of theft.
- Whenever available, use 2-factor authentication on all software or websites that require authentication (password + code sent by text message for example. This is in essence what banks require you to do in order to connect to your ebanking).
- Passwords should be: min. 12 char. long, a combination of numbers, letters, special characters, upper-case and lower-case.
- Do not use words, number, dates or phrases that are easy to guess or easily associated with you for your password.
- Create a password policy for your firm and have it enforced by your IT Specialist in all systems used by your firm's staff.
- If you procure new software or devices that have a default password on them, change that password to a compliant password before giving it to your staff.
- Do not share your passwords with anyone.



Mobile device security

Lawyers commonly use their personal mobile devices (laptops, cellphones, etc) to access professional emails and will inevitably store your law firm's documents, or at least some information related to cases, on these devices. These devices must be encrypted and protected by a secure password compliant with your firm's password policy.

- Mobile devices must have their security features enabled at all time.
- Lawyers should always have a pin number /password protection enabled - ideally 6 digits long at the very least.
- Lawyers should enable encryption of their device. Ask your IT Specialist to help you, if your are unsure whether your device is encrypted or not.

- Keep your mobile device updated at all times: run system and application updates as soon as they are available in your device settings or in your app store.
- Do not connect to public Wi-Fi.
- Ensure that you use a VPN* when sending sensitive data and that this data is encrypted.
- Ask your IT Specialist for help if in doubt.

* Virtual Private Network: allows you to securely transfer data from your computer or mobile device without the risk of interception.



Awareness

Users are the weakest link when it comes to cybersecurity. The best ways to reduce the risk they pose is through awareness and training. In this context, the responsibility of enforcing policies falls upon senior partners who MUST show the example. Associates and other staff will not enforce information security if senior partners do not show the example, or will fail to take information security seriously.

- Organize mandatory, regular awareness trainings for your staff with your Information Security Expert. There must be a periodic schedule for this training.
- Provide secure physical storage for your staff to lock sensitive documents and devices away when not in use.
- Periodically review your password policy and ensure that it is enforced by all, starting with partners - who are often the weak link.
- Users must also be provided with a list of dos and don'ts - e.g. no sharing of passwords with colleagues, lock computer when not in immediate use, clean desk policy, ...
- Educate users on how to identify phishing emails.
- Have a reporting process that users can follow if they notice suspicious activity or have doubts about an email.
- Create a process to handle unexpected email or phone requests, especially if they target key individuals with payment / confidential information / unusual requests.
- Inform your staff about new threats that emerge as soon as they emerge. Your Information Security Expert can alert you, if you ask him/her.





How to reduce my risk?

Although it is not possible to completely eliminate the risk, there are ways to mitigate it:

- **Social Media** : Secure your privacy settings. Although the information you put on social networks may seem harmless, it can be used by cybercriminals to understand your preferences, hobbies and routines. This data may easily be used against you. When posting information on social networks, restrict access to your friends or direct connections.
- **Use a VPN** : A VPN is a 'virtual private network' and should always be used when browsing the internet, checking emails or sending data. This is especially important if you connect to a public wi-fi. Ask your IT Specialist to set one up for you.
- **Passwords** : Passwords must be frequently replaced. Use a different passwords for each service you use and manage them with a password manager (see p. 13). Change the passwords every six months or if you suspect that it could have been compromised, or if you have shared it with someone. See also p. 9 for password creation guidelines.
- **Website Security** : When surfing the internet, check that the site's address starts with "https://". HTTPS indicates that the site you are on is probably safe and secure to use. If you need to shop online or otherwise transfer sensitive data online, make sure that the site address begins with HTTPS.
- **Links and Attachments** : When you download an attachment or click an unknown link, you risk infecting your computer with malware. When you receive a link or an attachment, check the sender's name and email before opening it. If you have any suspicion, do not open it and call the sender to check or contact your IT Specialist or your Information Security Expert.
- **Clean desk policy** : Confidential information should be stored away securely. Do not leave any passwords, confidential information or other sensitive data on your desk. When leaving your working place, lock your computer.
[Windows: window key + L]
[Apple: Control + Shift + Power]

USEFUL TOOLS

Password safes

SecureSafe - Swiss Service. SecureSafe creates strong passwords for you, stores them securely and allows you to easily retrieve them from your laptop, tablet or smartphone.

Bitwarden - A free and open source password manager. It aims to solve password management problems for individuals, teams, and business organizations.

1Password - Has an app for Windows, macOS, Android, and iOS. Secure yet simple authentication when adding new devices. Two-factor authentication. Extensions for most browsers.

File sharing

OnionShare - An open source tool that lets you securely and anonymously share a file of any size.

Nextcloud - Similar functionally to the widely used Dropbox, with the difference being that Nextcloud is free and open-source, and thereby allowing anyone to install and operate it without charge on a private server, with no limits on storage space or the number of connected clients.

CryptPad - A private-by-design alternative to popular office tools and cloud services. All the content stored on CryptPad is encrypted before being sent, which means nobody can access your data unless you give them the keys.





Email

Mozilla Thunderbird - A free, open source, cross-platform email, news, and chat client developed by the Mozilla Foundation. Thunderbird is an email, newsgroup, news feed, and chat (XMPP, IRC, Twitter) client.

Enigmail - A security extension to Thunderbird and Seamonkey. It enables you to write and receive email messages signed and/or encrypted with the OpenPGP standard.

Encryption

VeraCrypt - A source-available freeware utility used for on-the-fly encryption. It can create a virtual encrypted disk within a file or encrypt a partition or the entire storage device with pre-boot authentication.

GnuPG - A GPL Licensed alternative to the PGP suite of cryptographic software. GnuPG is compliant with RFC 4880, which is the current IETF standards track specification of OpenPGP. Current versions of PGP (and Veridis' Filecrypt) are interoperable with GnuPG and other OpenPGP-compliant systems. GnuPG is a part of the Free Software Foundation's GNU software project, and has received major funding from the German government.

Cryptomator - Free client-side AES encryption for your cloud files. Open source software: No backdoors, no registration.

DISCLAIMER

This brochure has been compiled for educational, informational and awareness raising purposes only. Information contained therein is not individual advice. It is instead intended to reflect information security standards and general practices. You have no obligation to implement or carry out any action, course of action, recommendation or anything else contained herein.

You should instead have your individual / your firm's individual situation reviewed and assessed by an information security expert. The Swiss LegalTech Association does not assume any liability of any kind for any loss, damage, prejudice or other harm in any way, shape or form, resulting from or in connection with the reliance on the information contained herein.

Software / company recommendations made in this brochure are equally given for information purposes only. The Swiss LegalTech Association does not endorse nor provide any kind of warranty in relation to these recommendations. We instead consider that readers should assess their individual needs in cooperation with their information security expert.

In general, this brochure is intended to underline the need to work with a qualified Information Security Expert and a qualified IT specialist.

Finally, this brochure is intentionally NOT exhaustive. It is only intended to provide a general overview of the topic.





SOCIAL NETWORKS

LinkedIn

[linkedin.com/company/10801496](https://www.linkedin.com/company/10801496)

<https://www.linkedin.com/groups/7061104/>

<https://www.linkedin.com/groups/8979895/>

Facebook

<https://www.facebook.com/swisslegaltech>

Twitter

<https://twitter.com/swisslegaltech>

YouTube

<https://www.youtube.com/channel/UC1H2vgAy1JpWJP8qu2TwLww>

WEBSITE

<https://www.swisslegaltech.ch/>

THE AUTHORS

Thando Toto, Cloud Security Specialist

Diogo Duarte, Legal Counsel

Nicolas Torrent, Lawyer, Managing Director
Digilegal.com, Vice-President Swiss LegalTech
Association