Information Security Policy

Version 5, September 2021

The AS&K Group includes all associated companies and subsidiaries, and will be referred to as the Company herein.

Introduction

The *Information Security Policy* covers our rules and requirements to ensure the security of our systems and the information stored and processed with them. It should be read in conjunction with our Policies on *Data Protection*, *Internet Acceptable Use*, and *Social Media*.

Information security is central to our business. We receive, store, use and generate information for the Company and on behalf of our clients, some of which is sensitive or confidential. We also occasionally handle personal data that falls under the provisions of GDPR, the Data Protection Acts or other privacy legislation. It is critical therefore that you understand the importance of information security and strictly adhere to the rules and procedures described in this document.

This Policy forms part of your contract of employment and breach of the Policy may lead to disciplinary action and, in serious cases, may entitle the Company to terminate your employment.

1. General Principles

1.1. You should treat all of the Company's information, whether it be electronic files, emails, print-outs, or printed materials, as private and confidential. It must remain secure at all times. This *Information Security Policy* describes the steps you must take, and the processes you must follow, to keep our systems and our information secure. In general, you must:

1.1.1. never divulge your passwords to anyone; you are responsible for keeping your passwords secure, and for updating them regularly as requested by our systems (see Paragraph 2);

1.1.2. keep your Company devices secure and up-to-date (see Paragraph 3)

1.1.3. be vigilant when receiving and reading emails and handling attachments (see Paragraph 7);

1.1.4. avoid using removable media or storage devices such as USB sticks unless authorised to do so (see Paragraph 8); and

1.1.5. keep printing out of documents to a minimum and put printed materials in the secure waste when finished (see Paragraph 9, 11).

2. Your Password And Network Identity

2.1. The Company uses Microsoft Active Directory (AD) to manage network identities. Your network identity, comprising your username and password, will allow you to log in to and access our network, Cloud systems, and software

2.2. Our AD password policy will automatically require you to set a strong password, and to change this password on a quarterly basis

2.3. You must keep your password secure. Do not divulge your password to anyone, even IT. Never write it down, either on paper or electronically. If you forget your password, IT can reset it for you

2.4. Our Office365 accounts use 2-factor authentication, and you will be required to set this up. You will need to authenticate on a second device via Microsoft Authenticator App when accessing Office365 software on a device for the first time.

2.5. The majority of our systems and software use AD authentication, either directly or via SSO. For the few that do not (e.g. PeopleHR), IT will create you an account using your Company email address as username and a temporary password that will require updating on first log in. These systems may also require a special link specific to you to access them; make sure you bookmark this link. You must:

2.5.1. set a strong password using a combination of caps and lower-case letters, numbers and special characters of at least 12 digits

2.5.2. keep this password secure as per the instructions in Paragraph 2.3; and

2.5.3. change it periodically as required by the system or instructed by IT; and note:

2.5.4. your account on these systems will be deactivated when you leave

3. Laptop Computers And Mobile Devices

3.1. You have been provided with a Company laptop computer. You may also have been provided with a mobile device (iPhone, iPad, etc.) if required for your role. It is your responsibility to maintain the security of these devices and protect them from theft, but they have been configured to be as secure as possible for you.

3.2. Appropriate software for your role has been installed on your laptop and will be managed by IT. If you require any additional software to be installed then you will need to submit a request to IT who will conduct a risk–benefit assessment and install it for you if appropriate (as you do not have the admin rights for your computer to install software yourself)

3.3. Appropriate software (for example, Microsoft Office Apps, Chime) has been installed on your mobile device. You may install other Apps on your device using your own personal credentials (e.g. AppleID) for personal use if you wish

3.4. Mobile Device Management (MDM) software has been installed on all Company devices to enable IT to remotely manage them. Note, this includes tracking the location of the device; you consent to this tracking as part of your terms of employment; this also provides IT the ability to remotely install updates and new software, and to wipe the device should it be lost or stolen

3.5. System and software updates will be applied automatically

3.6. On your laptop, antivirus software has been installed and will scan your hard drive periodically. Our email system also performs antivirus scanning on the server, before the email reaches your device (see Paragraph 7)

3.7. Your device(s) are encrypted, which means the information on them cannot be accessed or read by anyone that does not have the credentials to log in

3.8. Your laptop has been configured to require you to log in on start-up, wake from sleep and after 10 minutes of inactivity; if you need to change this (for example, to use as a presentation laptop in a meeting), speak to IT about doing this and the additional security steps you must take

3.9. Similarly, your mobile device has been configured to require your passcode on start-up, wake from sleep and after 30 seconds of inactivity

3.10. Always keep your password secure (see Paragraph 2)

3.11. If included, you may use the device's fingerprint reader (e.g. TouchID) or facial recognition software (e.g. FaceID) but you must never allow anyone else to add their biometric data (finger, face) to the system
3.12. Do not connect removable media or storage devices without permission from IT; this includes USB sticks and portable hard drives (see Paragraph 8)
3.13. Do not try to circumvent any of the security features of your device for any reason; this constitutes a serious disciplinary offense. If you have a problem, speak to IT.

4. Bring Your Own Device (BYOD)

4.1. The Company provides every employee with a laptop computer, and for some roles, a mobile device. These devices are controlled by the Company and IT via MDM software. BYOD refers to the use of personal devices such as laptops, tablets, and mobile phones, to access company systems, networks and Cloud services. There are security and data protection risks with allowing this, and given that all employees are provided with appropriate equipment, the use of such devices is not permitted
4.2. You may, in exceptional cases, access your email via Outlook Webmail from a non-company device, but in this case:
  4.2.1. you will be required to authenticate your login via 2FA, so you will require access to the second device you set up with the Microsoft Authenticator App
  4.2.2. do not download any email attachments to the non-company device
4.3. You may use the Guest WiFi network to access the Internet in our offices from your own devices; access to the Company WiFi network is restricted to Company devices via their MAC address.

5. Our Network

5.1. The Company's office has a local area network (LAN) that comprises devices (computers, printers, etc.) and servers connected via WiFi and ethernet. The network has access to the internet through our internet gateway, which is protected by a physical WatchGuard firewall.
5.2. Devices can access the LAN within the office by joining the WiFi network. Only devices with known MAC addresses can access the LAN. Do not attempt to connect other devices to the WiFi
5.3. Devices can also join the LAN from outside the office via the Company's virtual private network (VPN) connection. Speak to IT for help using this software
5.4. The network logs the activity of all devices connected to it, and these logs may be examined from time to time
5.5. Use of our internet connection is covered by the *Internet Acceptable Use Policy*; you should refer to this policy for guidance on internet use rules and best practice
5.6. Non-company devices, such as your personal devices and devices of visiting clients, may use the WiFi's guest network. This allows the device to connect to the internet without access to our LAN

6. Cloud Systems

6.1. The Company uses a number of Cloud-based systems, including Microsoft Office Applications and SharePoint Online. Access to the majority of these systems is controlled via AD or Single Sign-On (SSO)

6.1.1. For systems that do not have SSO, IT will create an account for you. You must keep your log-in credentials for these systems confidential (see Paragraph 2)

6.2. SharePoint Online has granular permissions and access features that control, via AD, who has access to particular areas, folders, and files, which the Company uses to protect the confidentiality of each of our clients' information, Company HR and financial information, and of personally identifiable information (PII) that we are required to protect by Data Protection legislation.

6.3. File transfer services, such as Box.net, Dropbox, and WeTransfer are a convenient way of exchanging files with clients, vendors and staff working remotely. But note:

6.3.1. The majority of our clients either have a subscription to one of the main file transfer services which they will require us to use; or they will have an in-house file transfer solution; and often use of other systems is against client policy, or access is physically blocked by their firewall. It is therefore important to check with a client before proposing to use a file transfer system

6.3.2. For clients and vendors that don't have their own system, the Company has a WeTransfer account that can be used when needed. Never transfer sensitive or confidential files using the Company's WeTransfer account, as the files are uploaded to the WeTransfer servers prior to them being made available for download, so security cannot be assured

6.4. Using Cloud software that has not been provided by the Company, such as Google Docs, or Cloud storage systems such as Google Drive or iCloud Drive, is not permitted.

7. Emails

7.1. Bear in mind that email is unencrypted and not a secure form of communication. If you need to send an email or attachment containing information that is confidential, privileged or commercially sensitive, then speak to IT about the best course of action, e.g. how attachments can be encrypted or password-protected

7.2. All incoming emails are automatically scanned before they are delivered (via Message Labs and also by Exchange Online). The software will check for viruses, and will also block unsolicited marketing email (spam) and emails which have potentially inappropriate attachments. If there is a suspected virus in an email that has been sent to you, the sender will automatically be notified and you will receive notice that the email is not going to be delivered to you

7.3. You should exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious (e.g. 'phishing' emails, which may seemingly be from people within the Company but in a strange style or from a non-Company email address, or may request confidential information or urgent payments of invoices). IT should be informed immediately if a suspicious communication or suspected virus is received

7.4. You must not email business documents to or from your personal email account. You may send documents to a client's personal email account if you have the client's

express written permission to do so. However, under no circumstances should you send any business sensitive or confidential documents to a client's personal email account, even if the client asks you to do so.

7.5. You should also refer to the *Internet Acceptable Use Policy* for further information about email etiquette and use of our email systems (e.g. for personal communications).

8. Removable Media and Storage Devices

8.1. No removable media or storage devices should be attached to the Company's systems without the prior approval of IT, including USB sticks, portable hard drives, phones, tablets and other media devices. But note:

8.1.1. for clarity, external displays, projectors, TVs, webcams, and conference microphones are not media or storage devices and are not included in this instruction; you may connect your device to displays, cameras and microphones as needed. Speak to IT if you need help with this; and

8.1.2. our devices no longer have CD-ROM or DVD-ROM drives for accessing removable media. If you need to access information stored on these types of media, speak to IT

8.2. IT will store and manage all removable media and storage devices. If you need to use such a device (e.g. for the convenience of exchanging documents at a conference, where WiFi access may be limited), you can obtain one from IT. This will be encrypted. You must

8.2.1. keep this device safe, treating it in the same way as you would a laptop or mobile device (see Paragraph 3)

8.2.2. not store any sensitive or confidential documents on it

8.2.3. return it to IT as soon as you have finished with it; IT will wipe the device after use, so make sure any important files are transferred to our systems first

9. Printers And Copiers

9.1. The Company's offices have several multifunctional printer/copier/scanner devices. Use of these is controlled by software that requires you to input a pin to retrieve your printing. Speak to IT if you need help with this.

9.2. Do not leave printed documents on or near the printer; take them, use them, and then dispose of them in the confidential waste

9.3. We have a 'host desk' policy; all printed materials should be put in the confidential waste at the end of the day, or if still needed, locked in your locker.

9.4. Do not take print-outs home

10. Physical Building Access

10.1. Physical access to our premises is controlled by an NFC entry system. You will be issued a keyfob to gain entry. This fob is registered to you, and it is your responsibility to keep it safe:

10.1.1. attach the keyfob to a keyring or lanyard and keep it on your person at all times (for security, and to avoid getting locked out);

10.1.2. do not leave it on an unattended desk;
10.1.3. do not lend it to anyone;
10.1.4. if you have forgotten to bring your fob to the office, a spare can be signed out for the day; contact the Office Manager; and
10.1.5. if you lose the fob or if it is stolen, report this immediately to the Office Manager and to IT, who can disable the fob

10.2. If you plan to arrive early or stay late, you will need to have your fob updated to also be able to set and unset the building alarm, and you will need a shutter key for the front door. Speak to the Office Manager for this.

10.3. Note: the system logs the use of each key fob, so your entry and exit to the building and internal areas will be recorded; the logs may be examined from time to time

11. Working Remotely

11.1. This part of the policy applies to your use of our systems and equipment whenever you are working on the Company's business away from the Company's offices (i.e. working remotely, either at home or on-site).

11.2. When you are working remotely you must:

11.2.1. position yourself so that your work cannot be seen by any other person;
11.2.2. use a privacy filter for your laptop screen whenever you're in a public space;
11.2.3. not leave your laptop or mobile device unattended; your laptop will enter a screensaver with password if not used for 10 mins; but you should keep the lid shut when not in use, which will return it to the login screen;
11.2.4. take reasonable precautions to safeguard the security of your laptop and mobile device;
11.2.5. keep your password secret (see Paragraph 2);
11.2.6. inform the police and IT as soon as possible if any of your equipment has been stolen; and
11.2.7. ensure that any work that you do remotely is saved on the Company's Cloud systems or is transferred to our systems as soon as reasonably practicable (e.g. if you have had limited internet access)

11.3. Our main file repositories, SharePoint Online and OneDrive, are Cloud based services with access controlled via your AD credentials and accessible via a browser or App. If you need remote access to our legacy file servers, you will need to connect via our VPN. Speak to IT for help with this

11.4. You should start a VPN connection before joining any public WiFi network, as these are often insecure and easily spoofed

11.5. Avoid as far as possible printing out materials. If you do need to print something, it should be kept securely only for as long as necessary and shredded or disposed of in confidential waste immediately thereafter. Never print any sensitive or confidential information, or materials containing personal data, when working remotely

12. Compliance With Data Protection Legislation

12.1. You may occasionally be involved in processing personal data for the Company as part of your job. Data protection is about the privacy of individuals, and is governed by

the General Data Protection Regulation (GDPR) and the Data Protection Act 1998 & 2018 in the UK, and other legislation worldwide. Whenever and wherever you are processing personal data for the Company, you must keep them secret, confidential and secure, and you must take particular care not to disclose them to any other person (whether inside or outside the Company) unless authorised to do so. Further information on our rules and requirements for data protection is given in the *Data Protection Policy*.

13. Compliance With This Policy

Failure to comply with this policy may result in disciplinary action being taken against you under the Company's disciplinary procedures, which may include summary dismissal. If there is anything in this policy that you do not understand, please discuss it with your line manager.

Please note that the procedures and policies outlined in this policy document, and in any related policy, may be reviewed or changed at any time. You will be alerted to important changes, and updates will be made available.

Policy edition: February 2007 // Revised May 2012 // Revised August 2016 // Revised March 2018 // Revised September 2021

Declaration

I have read the Company's *Information Security Policy*.

I acknowledge that the equipment with which I have been provided (and any software included) has been made available to me by the Company solely to assist me in the performance of my duties within the Company. It remains the property of the Company at all times.

I accept personal responsibility at all times for this equipment and any software included. In doing so, I agree to take all reasonable measures to protect this equipment (and software) from theft or unauthorised use; to keep it in proper working order; and to protect it against computer viruses.

I accept and understand that this declaration and the *Information Security Policy* form part of my terms and conditions of employment and hereby agree to abide by the terms laid out therein.

Name:

Signed:

Date: