INFORMATION SECURITY AWARNESS DECLARATION

Information security (sometimes shortened to InfoSec) is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic or physical). For us here at Startek, that means protecting our customers data with strong security measures, and being aware of our responsibilities, regardless of your role.

General Computer Controls (Strong/Weak Controls)

Controls are the measures we put in place to minimize our exposure to information security risks. The types of controls you can implement in your client area might be:

- A strong password
- Keeping a workstation free of written documentation, customer records or data
- Ensuring your access to client data is only accessible by you. No sharing of passwords!
- Disposing of confidential records
- Storing information securely. Following ID and verification processes on every call or email where required.

Security Knowledge

Internet access is an integral component of our business here at Startek. However, such access does introduce the possibility of malicious attacks on our data and networks from anywhere on the planet.

To safeguard from such threats, Startek staff are required to have **adequate security awareness to ensure they understand the potential risks to the company** and its customers, and that poor security knowledge and practice can result in:

- Identity theft
- Monetary theft
- Legal ramifications (for yourself, Startek or its clients)
- Termination if company policies are not followed

Confidential information

Confidential information is any information considered to be private and sensitive. Some examples you might encounter in your client area are:

- Protected personal information about a client or customer
- Banking information
- Credit card information
- Financial records
- Passwords, PIN numbers, or other security codes
- Internal communications between Startek and a customer
- Various customer records related to their business dealings with us

Confidential information can be stored in many forms. It can be information printed on paper; data files stored on a computer or a hand-held device such as a laptop or smartphone; or recorded spoken word such as in a voice mail.

"Regardless of the form it takes, you are responsible to protect it from unauthorised disclosure or modification."

How to Protect Confidential Information

- Use only approved procedures when handling confidential information, especially when using the internet, email, or even voice communications.
- Your supervisor or the IT department can provide specific guidance on how to properly handle confidential information.
- If you are unsure of any procedures, ask your manager to guide you or see our policies on **SAFI**

User Ids

- Your user ID uniquely identifies you. You are responsible for all actions associated with your user ID; therefore, it is important to ensure that your user ID is used only by you and no one else.
- You will be held responsible for the actions of another individual if you allow them to obtain and use your user ID and password, or allow them access to any information in a client application while you are logged in with your ID.

Password Protection

Protecting your password is a critical factor in protecting confidential information; therefore passwords should be:

- Memorised and never written down in such a way that others can see or use them
- Kept a secret from others
- Be aware of scams to trick you into disclosing your password through anonymous phone or email
- Under no circumstances should anyone ever ask you for your password, or should you voluntarily give it out if asked
- Likewise, you must not attempt to learn another person's password and/or access another person's account using their password.
- Care should be taken when selecting a password. A poorly chosen password compromises security. Create a "strong" password by following these simple rules:
    - It must be at least eight characters in length, and in some areas of the business it must be at least ten characters in length *(Tip: The longer your password is, the harder it is to break)*
    - Use at least one upper case and one lower case letter
    - Use at least one number
    - Use at least one special character such as * ? # @ & $
    - Avoid using common words that can be easily guessed
    - Avoid using personal information such as your child's name, favorite sports team or pets.
    - Our systems at Startek will require you to change your login in password regularly to ensure we maintain information security.

Your Computer Workstation

- It is your responsibility to **log off or lock your computer** workstation whenever **leaving it unattended**, so that any confidential information on screen **cannot be seen by others.**
- It is recommended to log off your workstation when you are leaving your work area at the end of your shift.
- Leaving a workstation logged on and unattended could **lead to an unauthorised access of confidential information.**

Personal Usage

- Startek computer systems are intended to be used for **business purposes only.**
- Limited personal may be permissible with **approval by your supervisor** and is on **your own personal time.**
- Startek provides a limited number of computers that can be used for personal internet browsing outside of your work area I.e. in the breakout areas on each floor.

EMAIL

- Organizational email is limited to authorized users and is for conducting official Startek communications. Personal use of company email is not allowed.
- You are responsible for all activity on your assigned email account. **Don't share your password with anyone.**
- Keep communications with Startek customers formal and friendly.

INTERNET

- Internet access is provided to Startek staff based on **legitimate business needs**.
- All internet access from all company workstations is logged and monitored by IT.
- Restrictions to access to non-work related, objectionable or malicious sites is enforced by IT.
- **The ability to connect with a specific website does not in itself imply that access is allowed.** If you discover that you have inadvertently connected to an inappropriate website please disconnect from that site and notify the IT Service Desk.

Inappropriate Activity

- Under no circumstances should organization-owned systems be used for gambling, personal profit, or to download, distribute materials, comments, pictures, or other forms of communication of a sexual nature or which are otherwise obscene, intimidating, offensive, or create a hostile work environment.
- **The violation of above mentioned rules may lead to disciplinary action not only including termination, but also subject to applicable laws involving civil and/or criminal penalties for violations with regard to inappropriate access or disclosure of private or confidential data or information.**

Social Engineering

- Social engineering is the practice of obtaining confidential information by manipulation of legitimate practices. A social engineer will commonly use the telephone or internet to trick people into revealing sensitive information or getting them to do something that is against typical policies.
- Social engineers exploit the natural tendency of a person to trust another's word, rather than exploiting computer security holes.
- Social engineers might attempt to:
    - ✓ Try to persuade you to **disclose personal information** about someone they have no right to i.e. they may claim to be related to, the spouse of or have some other emergency reason for obtaining the data.
    - ✓ Pose as members of an organization that claims rights to data
    - ✓ Offer bribes or coerce

Avoid Being a Social Engineer Victim

- If an unknown individual claims to be from a legitimate organisation, **try to verify his or her identity directly with the company before beginning dealings with them.**
- Do not provide personal information or information about your client area unless you are **certain of a person's authority to have the information**. If in doubt, **escalate the call to your supervisor.**
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a link or web site connected to the request.

Phishing

- Phishing is a form of social engineering. Phishing attacks use email or malicious websites to obtain personal information by posing as a trustworthy organization.
- For example, a caller may seemingly be from a reputable credit card company or financial institution that requests account information on one of your customers, often suggesting that there is a problem or it is an emergency. They may even advise the customer has already authorized them.
- Always follow your ID checks as required by your business on every call.

How Can I Safeguard Against Phishing?

- Don't reply to email or pop-up messages that ask for personal, financial or organizational information on our systems here at Startek.
- Look out for a sender's email address that is similar to, but not the same as, a company's official email address.
- **Don't share your Startek / Client email address with an organisation you can't verify.**
- Fraudsters often send thousands of phishing emails at one time. They may have your email address, but they occasionally have your name. Be doubtful of an email sent with a generic greeting such as "Dear Customer" or "Dear Member".
- Never submit confidential information via forms embedded within email messages.
- Don't click on links in email or instant messaging, and never use links in an email to connect to an external web site unless you are **sure the address is safe.**

IT SECURITY DO's & DON'Ts

DO's :

- ✓ Store all data and files on a network shared drive so that it can be backed up if necessary, and cannot be lost if your computer breaks or is stolen
- ✓ Password should be changed at least **once in every 45 days**
- ✓ Be extra careful when required to enter your password on a stranger's computer
- ✓ **Lock your computer while you are not working** (by pressing ALT+CTRL+DEL)
- ✓ Be cautious when opening attachments from strangers
- ✓ **Maintain a clear desktop / Follow all processes to ensure compliance** with PCI where relevant
- ✓ Deposit unwanted papers containing personal/customer information into shredding or recycling bins provided
- ✓ Be cautious while discussing, receiving or forwarding proprietary information
- ✓ Printing, photo copying or faxing is used and limited for legitimate business needs only
- ✓ Internet should be used for **business purposes only** i.e. responding to inbound customer emails for your client area
- ✓ At the end of your shift, ensure any papers or documents are disposed of or stored securely.
- ✓ Sensitive or classified information, when printed, should be cleared from printers and/or fax machines immediately
- ✓ Leave devices capable of recording or capturing customer data away from the operations floor.

DON'Ts :

- ✓ Never share your passwords with anyone
- ✓ Never leave your computer unlocked when you are away from your desk
- ✓ Do not keep computers online when not in use (Lock it while going on breaks & Logoff when the shift ends)
- ✓ Never send personal information about yourself or a customer (including names, account numbers, addresses, phone numbers or passwords) to strangers
- ✓ Do not write your password down anywhere
- ✓ Do not share your access with anyone
- ✓ Do not save your password on your system
- ✓ Do not gossip or share with others, sensitive information that you have access to
- ✓ Do not throw confidential reports in to the rubbish bin without shredding them
- ✓ Do not save files on the local desktop or hard drive of your computer
- ✓ Do not install unauthorised software or attach unauthorised hardware devices
- ✓ Do not access or download content not required or related to Startek
- ✓ Call centre staff are not to carry any mobile phones on the Operations floor
- ✓ Use of any portable storage device or media (e.g. USB sticks CD/DVD ROMs, compact cameras) is prohibited in production area.
- ✓ Do not send any chain emails or jokes, and do not subscribe to any non-work related (e.g. humour, pornography, news) mailing lists
- ✓ Do not send greetings to large distribution lists. Attaching multimedia files with greetings is prohibited
- ✓ Do not upload Startek data to the internet (including sending such documents by email without the prior approval of your manager)
- ✓ No attachments can be viewed or downloaded from the personal email sites

- ✓ Do not send credit card, ATM or electronic funds transfer information over the internet
- ✓ Playing songs, video, software, games or viewing images, files not meant for official purpose are prohibited. Also running any non-standard and unapproved software even for official purposes is prohibited.
- ✓ Do not enter company facilities without ID cards displayed at all times, or refuse to show them to security personnel whenever asked
- ✓ Photographic equipment is prohibited in Startek premises (without prior approval)
- ✓ All personnel are guided not to repair, change or relocate their computer by themselves. The IT Service Desk must be consulted for any assistance.

Reporting Security Incidents

Notify IT and your supervisor if you become aware of or suspect the following:

- ✓ Theft of or damage to IT equipment
- ✓ Unauthorised use of a user's password
- ✓ Policy violations
- ✓ Usage of gadgets, mobile phones and/or cameras, USB hard drives or other media storage devices in the production environment
- ✓ Any other problems or questions with information security or privacy.

You can also call the IT Service desk on (03) 9256 5034 or send an email to servicedesk@au.aegisglobal.com or information.security@aegisglobal.com to register any security concern or incident.

The internet security policy can be found on Safi!
HELP -> Human Resource -> HR policies

Employee Declaration

Name : MOHD SAIF KHAN

Emp. Code : _____

Department : _____

I understand that as an employee of Startek Services Australia, my actions and behavior are governed by range of legislation and policies as amended from time to time

I hereby confirm that I have read and understood my rights and responsibilities related to Startek' policies on Information Security. I am aware that breaching this policy could result in any one of the following ramifications: informal chat, informal warning, final warning or dismissal.

I am committed to perform my duties and drive a culture of security in our organization at all times. This also extends to any Startek sponsored or employment related situation such as training courses, promotional events, Christmas parties, whether outside working hours or at another site.

Employees Signature : MOHD SAIF KHAN

Date : 20/05/2022