

Data Privacy Compliance for Small Business Owners

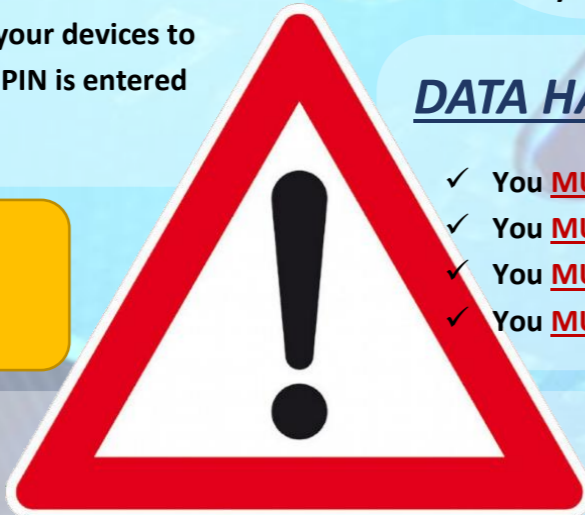
GENERAL COMPLIANCE

- ✓ Do all things necessary to ensure that personal data is kept secure at all times.
- ✓ Remain alert and aware of threats at all times.
- ✓ Keep up to date on security threats, subscribe to security alerts and keep your computer secure and up to date using the latest updates and patches.

USER ACCESS MANAGEMENT

For all computer equipment, including laptops and tablets and mobile phones...

- ✓ You **MUST** use a password on your devices.
- ✓ You **SHOULD** use two-factor authentication if possible.
- ✓ You **MUST** configure your devices to automatically lock after 30 minutes of inactivity and require a password to reactivate.
- ✓ You **MUST**, where possible, configure your devices to lock for 30 minutes if the password or PIN is entered incorrectly 5 times.



PASSWORDS AND PINS

Make sure that your passwords and PINS use these simple rules...



- ✓ Your password **MUST** be kept secret and **NEVER** given to anyone EVER! There is **NEVER** a reason that someone will need it or ask you, unless they are up to no good!
- ✓ Your password **MUST** be **EASY** to remember but **HARD** for someone else to guess.
- ✓ You **MUST** change your password at least every 90 days.
- ✓ You **MUST** use a **UNIQUE** username and password combination for each device and website.
- ✓ You **MUST**, use A-Z, a-z, 0-9 and at least one special character when creating a **STRONG** password.
- ✓ You **SHOULD** use a complex Pass-Phrase rather than a password. *Like This1s@5trongP@\$5w0rdPhr@5e*
- ✓ You **MUST NOT** write your passwords down.
- ✓ You **MUST** use a PIN or biometric lock for your mobile phone.

DATA HANDLING

- ✓ You **MUST NOT** share our data with anyone else
- ✓ You **MUST** only do the task assigned with the data
- ✓ You **MUST NOT** make unnecessary copies
- ✓ You **MUST** destroy any of our data when requested to do so.

EMAIL AND WEBSITES

- ✓ You **MUST NOT** open attachments on email that you weren't expecting.
- ✓ You **MUST NOT** click on links in emails that you weren't expecting.
- ✓ You **MUST NOT** do work on a browser without a **VALID** SSL Certificate.
- ✓ You **SHOULD** have a different email account for private and work purposes.
- ✓ Your work email messages **MUST** be stored using encryption.

COMPUTERS AND DEVICES

Keeping your devices secure is critical for Data Privacy Compliance.

You **MUST** keep your devices updated and keep all the threat management software applications updated and active.

- ✓ You **MUST** use up to date firewall software.
- ✓ You **MUST** only install software from credible sources.
- ✓ You **MUST** use ANTI-VIRUS software.
- ✓ If your Anti-Virus detects a threat, it **MUST** be quarantined.
- ✓ You **MUST** use disk encryption software on all disk drives.
- ✓ If you use a USB drive, it **MUST** have data encryption on it.
- ✓ You **MUST** use a software threat management system like Microsoft® Defender®
- ✓ Your Anti-Virus, Anti-Malware, System Updates and Firewall software **MUST** be updated regularly and if possible **AUTOMATICALLY**.
- ✓ Your devices **MUST** be backed-up regularly (at least once a week) using a password to secure and encrypt the backup.
- ✓ You **MUST** be the only person who can access your back-ups.
- ✓ You **SHOULD** verify your back-ups if that option exists in your software.
- ✓ You **MUST** only use reputable cloud service providers that have recognised data privacy policies like ISO 27001 or ISO 9001.
- ✓ You **MUST NOT** connect your computer to Free or Public Wi-Fi when you are doing work for us.
- ✓ You **SHOULD** choose quality software applications from reputable developers like Google® and Microsoft®.
- ✓ You **MUST** keep all Routers, Wi-Fi, Modems or other network equipment in your home or office secured with a password and encryption.
- ✓ You **MUST** only use recognised and authorised repairers for your devices if they are damaged.
- ✓ You **MUST** always ensure that personal information on your devices is secured at all times!
- ✓ You **MUST** "Factory Reset" all devices before you dispose of them.

Check off each item as you work through this list...

INCIDENT MANAGEMENT

You **MUST** tell us if any of these things happen to you so we can help you to minimise the impact of the incident, loss or theft of your devices.

It allows us to shutdown your access until the incident is resolved and make sure that people's private details remain safe and secure. This allows us to keep your details secure too.

You **MUST** tell us **IMMEDIATELY** if your device is...

- ✓ Infected with a Virus that you can't remove.
- ✓ Hacked or otherwise compromised.

You **MUST** tell us **IMMEDIATELY** if you believe that you have become the victim of a Phishing attack.

You **MUST** tell us if a device that you use to do work with us is lost or stolen as soon as possible.

You **MUST** tell us if a Service or Website that you use to do work with us is compromised.