Security Measures for Your Business

This quick look security guide covers the key security points that you need to be aware of as part of your commitment to data security.

This security guide is specific to your business because you use devices or systems in your business that are connected to the internet.

You must confirm that you agree with all of the statements in this guide. If you do not agree with any statement, then you will need to get in touch with us so that we can help you to reduce your risk.

Keep a copy of this guide on your business premises so that all staff members have access to it.

Share this guide with all staff members in your business that handle your customers' payment card details so they are aware of what they need to do to keep your customers' payment cards safe. Sign your copy and make sure that all staff members sign their copy too. These signed copies must be kept on file at all times.

Every year we ask that you go through this list with all members of staff in your business as a refresher and that you update the signed copies each year.

Signed _____ Date _____

Quick tip

Cardholder Data – this is the information on a payment card needed to make a card payment.

Sensitive Authentication Data – is all of the elements of a payment card used to verify the identity of the cardholder. This includes the data contained on the cards magnetic stripe or chip, the card security number (which is the three-digit or four-digit number printed on the card) and the cardholder's PIN and 'PIN block'.

Secure and protect payment card data

☐	My business collects or captures cardholder data and/or sensitive authentication data only when and where it really is needed.
☐	My business does not keep or store cardholder data after the initial transaction.
☐	My business does not keep or store sensitive authentication data after the initial payment transaction has been processed.
☐	Any cardholder data that my business has a need to keep is protected at all times. We make sure that cardholder data cannot be accessed by people that have no need to see or view the data.
☐	My business has a 'clear desk policy' to make sure that people put away documents that may contain sensitive or cardholder data when not at their desk or work station.
☐	All cardholder data and sensitive authentication data collected is destroyed securely or erased once it is no longer needed for a business reason.
☐	We destroy or erase cardholder data and/or sensitive authentication data using methods that make sure the information cannot be reconstructed or recovered.

Use a firewall to protect your business network

☐	My business uses a firewall to protect the internal business network from the internet
☐	My business uses a firewall to protect the internal business network from other less trusted networks, such as guest wireless networks or business partner/supplier networks
☐	My firewall only allows the necessary traffic in to and out of the business network.
☐	A personal firewall software (or equivalent protection) is installed on all laptops and other mobile devices that are used on our business network.

If wireless networks are used by your business you need to make sure they are secure

☐	Any wireless network that is accessible to the public (e.g. a guest Wi-Fi network) is kept completely separated from any wireless networks used by my internal business network.
☐	The wireless access point/router's default ('out of the box') settings, including all pre-set passwords have been changed.
☐	All wireless networks used by my business are set-up so that they use strong wireless authentication and encryption. My business does not use WEP for encrypting wireless networks.

Secure remote access to your business network

☐	My business only allows authorised personnel to have remote access to my business network. This may include employees, third party vendors or IT support providers that specifically need remote access.

☐	The personnel with remote access can only gain access to the specific systems, applications, and information on my business network that is required for them to do the work needed.
☐	All remote access methods use strong encryption to secure the remote access and protect the data that is being sent.
☐	All remote access methods use multi-factor authentication. Multi-factor authentication requires the remote user to prove their identity using at least two forms of unique authentication
☐	All third party vendors or IT support providers with remote access to my business network use authentication credentials that are different to those used for access to any of their other customers

Use approved payment devices and applications

☐	My business only uses PCI approved card readers and PIN entry devices. These devices are included on the list on the PCI DSS website, link below: https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
☐	If my business uses payment application software, I have confirmed that the software has been validated against the Data Security Standard for Payment Applications (PA-DSS) and can be found on this list: https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications?agree=true *PA-DSS validation is not applicable for custom/bespoke payment applications, Software as a Service web applications, web-based hosted payment pages or Virtual Terminals

Protect your systems by configuring them securely

☐	The computers, servers, applications and network devices (including firewalls and routers) on my business network are properly and securely configured. My business has removed or disabled unnecessary software and functions.
☐	All unnecessary user accounts have been removed or disabled.
☐	Any default or 'pre-set' passwords for user, administrative or system accounts have been changed.

Protect your systems by keeping them up to date

☐	The operating systems and software on the systems, computers and devices used by my business are kept up-to-date
☐	The operating systems and software used by my business is supported by the vendor or supplier
☐	Personnel in my business periodically check for the release of new security patches.
☐	Personnel in my business make sure that security patches are installed in a timely manner

Protect your systems from malicious software

☐	All computers, servers, PCs, laptops and mobile devices used by my business are running anti-virus and malware protection software
☐	The anti-virus / malware protection software is set to update automatically
☐	The anti-virus / malware protection software is set to regularly run full system scans

Protect your business by controlling access

☐	Users only have the access and privileges to systems and data that they need to do their job

☐	Each user has their own individual login (accounts) and password for accessing my business network and systems
☐	My business separates administrator and user logins (accounts)
☐	Administrative rights have only been given to delegated personnel who need the extra level of access and rights to be able to do their job.
☐	The rights of 'normal' users are limited so that they cannot make unauthorised changes to or install software on my business systems.
☐	Access to my business network and systems is removed for personnel on the termination of their employment or contract.

Protect your business by enforcing a password policy

☐	All default and pre-set passwords on hardware, software and other systems and devices used by my business have been changed
☐	Passwords are kept confidential. Users in my business know not to share their passwords
☐	Users of my business systems, including staff, contractors and service providers, are required to choose strong passwords
☐	Users are required to change their passwords regularly
☐	Users of my business systems know to avoid using the same password more than once

Protect your business by controlling physical access

☐	My business premises and location(s) are kept secure. Only authorised personnel can access any non-public areas.
☐	My business has access controls in place to make sure that unauthorised persons do not have physical access to any of our business computers, servers or systems.
☐	Each of the card readers and PIN entry devices at each point-of-sale are checked regularly to make sure that they have not been tampered with or been replaced with a fraudulent device.

Raise security awareness

☐	My business has an information security policy that lets my staff know what they need to do to keep my customers' payment card data safe.
☐	All employees and personnel in my business have been brought through the company information security policy. They understand their role and the responsibility they have in protecting customer cardholder data.
☐	My business uses induction or orientation sessions to make sure that all new hires, temporary staff and contractors are made aware of the security policies in place
☐	My employees are periodically reminded of their security responsibilities

Plan of action in the event of a security incident or breach

☐	My business is prepared in case of a security incident or data breach.
☐	My business has a security incident response plan to help us respond quickly and effectively should the worst happen.
☐	My security incident response plan covers the various types of incidents that my business may be subject to.
☐	The people working for my business (whether staff or third party providers) know to report anything that does not seem right.

Additional notes: