INFORMATION SECURITY

January 3, 2018 v2.2

ABSTRACT

Assess your compliance with data protection in the specific areas of information and cyber security policy and risk, mobile and home working, removable media, access controls and malware protection.

Admin-PC

[Course title]

Overall rating

Your overall rating was green.

- 0: Not yet implemented or planned
- 4: Partially implemented or planned
- 13: Successfully implemented
- 2: Not applicable

AMBER: partially implemented or planned

Your business has established a process to identify, assess and manage information security risks.

Your business ensures information security risks are assessed and appropriately managed.

Areas for focus/suggested actions

Where measures have only been partially implemented, please select the appropriate actions from the detail below:

Before you can establish what level of security is right for your business you will need to review the personal data you hold and assess the risks to that information. You should:

- consider all processes involved as you collect, store, use, share and dispose of personal data; and
- consider how sensitive or confidential the data is and what damage or distress could be caused to individuals, as well as the reputational damage to your business, if there was a security breach.

With this clearer view of the risks you can then implement the following:

- document your information risk management process in an information risk policy;

- ensure that you create either a stand alone information risk register or incorporate information risks in a central risk register; and
- regularly assess and update, treat, tolerate, or mitigate risks as appropriate.

Guidance

- Information risk management regime, in 10 steps to cyber security, National Cyber Security Centre

Your business has defined and allocated information security responsibilities.

Your business has established a management framework to coordinate and review the implementation of information security.

Areas for focus/suggested actions

Where measures have only been partially implemented, please select the appropriate actions from the detail below:

Without clear accountability for the security of systems and specific processes, your overall security will not be properly managed or coordinated and will quickly become flawed and out of date. You should:

- identify a person or department in your business and assign day-to-day responsibility for information security;
- ensure they have the necessary authority and resources to fulfil this responsibility effectively; and
- for larger organisations, appoint 'owners' with day-to-day responsibility for the security and use of business systems.

Guidance

- Information security, ICO Guide to data protection

Your business has established a mobile working policy.

Your business ensures the security of mobile working and the use of mobile computing devices.

Areas for focus/suggested actions

Where measures have only been partially implemented, please select the appropriate actions from the detail below:

Mobile working can involve the storage and transit of personal data outside the secure boundaries of your business. However, mobile computing devices (for example, laptops, notebooks and smartphones) are vulnerable to theft and loss, and there are confidentiality risks when using devices in public places. Therefore, you should:

- assess the risks of mobile working (including remote working where mobile devices can connect to the corporate network);
- establish a mobile working policy (based on the outcomes of the risk assessment) to assist in ensuring the security of mobile working and the use of mobile computing devices;
- implement a process that sets out procedures to follow for authorising and managing mobile working; and
- keep a log of all mobile devices used in your organisation and who they are allocated to.

Guidance

- Home and mobile working, in 10 steps to cyber security, National Cyber Security Centre
- Bring your own device (BYOD), ICO

Your business has established a process to ensure software is kept up-to-date and the latest security patches are applied.

Your business prevents the exploitation of technical vulnerabilities.

Areas for focus/suggested actions

Where measures have only been partially implemented, please select the appropriate actions from the detail below:

Most popular software products contain technical vulnerabilities that can be exploited by attackers to gain unauthorised access to personal data held in your systems. You should:

- use the latest versions of operating systems, web browsers and applications; and

- ensure these are updated regularly to help prevent the exploitation of unpatched vulnerabilities.

Guidance

- Patch management, in Cyber security essentials, GOV.UK website
- Software security updates, in Protecting personal data in online services, ICO

GREEN: successfully implemented

- ✓ Senior management has approved and published an appropriate information security policy.
- ✓ Your business provides management direction and support for information security in accordance with business needs and relevant laws and regulations.
- ✓ Your business has established written agreements with third party service providers that include appropriate information security conditions.
- ✓ Your business ensures the protection of personal data that is accessed by suppliers and providers.
- ✓ Your business has established a process to report and recover from data security breaches.
- ✓ Your business ensures the management of data security breaches, including communication of information security events and weaknesses.
- ✓ Your business has established regular information security awareness training for all staff.
- ✓ Your business ensures that employees and contractors are aware of and fulfil their information security responsibilities.
- ✓ Your business has established entry controls to restrict access to premises and equipment on a need-to-know basis.
- ✓ Your business prevents unauthorised physical access, damage and interference to personal data.
- ✓ Your business has established secure storage arrangements to protect records and equipment.
- ✓ Your business prevents loss, damage, theft or compromise of personal data.
- ✓ Your business has established a process to configure new and existing hardware to reduce vulnerabilities and provide only the functionality and services required.
- ✓ Your business has established controls to manage the use of removable media.
- ✓ Your business prevents unauthorised disclosure, modification, removal or destruction of personal data stored on media.

- ✓ Your business has established a process to assign user accounts to authorised individuals, and to manage user accounts effectively to provide the minimum access to information.
- ✓ Your business limits access to personal data held in information systems.
- ✓ Your business has established appropriate password security procedures and 'rules' for information systems and has a process in place to detect any unauthorised access or anomalous use.
- ✓ Your business has established effective anti-malware defences to protect computers from malware infection.
- ✓ Your business ensures that personal data is protected against malware.
- ✓ Your business has established a process to log and monitor user and system activity to identify and help prevent data breaches.
- ✓ Your business records events and generates evidence.
- ✓ Your business has established boundary firewalls to protect computers from external attack and exploitation.
- ✓ Your business ensures the protection of personal data in networks.

Not applicable

- ✓ Your business has established a process to securely dispose of records and equipment when no longer required.
- ✓ Your business has established a process to routinely back-up electronic information to help restore information in the event of disaster.
- ✓ Your business ensures protection against the loss of personal data.
