Minimum Cyber Security Standard

This is the first technical standard that will be incorporated into the Government Functional Standard for Security once published

Definitions:
"Shall" means that there is an obligation to perform the activity, without exception.
"Should" means that there is an expectation that the activity will be performed. There can be rare exceptions when the activity is not performed. However there must be a clear process in place to manage any risks.
"Users/Individuals/Administrators" also refers to staff, employees and contractors.
"**Departments**" also refers to organisations, agencies, Arm's Length Bodies and contractors.

Purpose:

The HMG Security Policy Framework (SPF) provides the mandatory protective security outcomes that all Departments are required to achieve. This document defines the minimum security measures that Departments **shall** implement with regards to protecting their information, technology and digital services to meet their SPF and National Cyber Security Strategy obligations.

As far as possible the security standards define outcomes, allowing Departments flexibility in how the standards are implemented, dependent on their local context. The definition of 'sensitive', 'essential', 'important' and 'appropriate' are deliberately left open, so that Departments can apply their own values based on their particular circumstances, however Departments are accountable for the effectiveness of these decisions and they **shall** reflect the HMG Government Security Classifications Policy[1] where relevant.

Compliance with the standards can be achieved in many ways, depending on the technology choices and business requirements in question. For Digital Services, this set of standards is complementary to the Digital Service Manual.

The standard presents a minimum set of measures and departments **should** look to exceed them wherever possible. Over time, the measures will be incremented to continually 'raise the bar', address new threats or classes of vulnerabilities and to incorporate the use of new Active Cyber Defence measures that Departments will be expected to use and where available for use by suppliers.

[1] The HMG Government Security Classifications Policy describes how Government classifies information assets and applies to all information that Government processes to deliver services and conduct business, including information received from or exchanged with external partners.

1	**IDENTIFY** ***Departments shall put in place appropriate cyber security governance processes.***	a) There **shall** be clear lines of responsibility and accountability to named individuals for the security of sensitive information and key operational services. b) There **shall** be appropriate management policies and processes in place to direct the Departments overall approach to cyber security. c) Departments **shall** identify and manage the significant risks to sensitive information and key operational services. d) Departments **shall** understand and manage security issues that arise because of dependencies on external suppliers or through their supply chain. This includes ensuring that the standards defined in this document are met by the suppliers of 3rd party services. This could be achieved by having suppliers assure their cyber security against the HMG Cyber Security Standard, or by requiring them to hold a valid Cyber Essentials[2] certificate as a minimum. Cyber Essentials allows a supplier to demonstrate appropriate diligence with regards to standard number six but the Department **should**, as part of their risk assessment, determine whether this is sufficient assurance. e) Departments **shall** ensure that senior accountable individuals receive appropriate training and guidance on cyber security and risk management and **should** promote a culture of awareness and education about cyber security across the Department.
2	**Departments shall identify and catalogue sensitive information they hold.**	a) Departments **shall** know and record: I. What sensitive information they hold or process II. Why they hold or process that information III. Where the information is held IV. Which computer systems or services process it V. The impact of its loss, compromise or disclosure

[2] Cyber Essentials helps guard against the most common cyber threats and demonstrates a commitment to cyber security. It is based on five technical controls but does not cover the entirety of the HMG Cyber Security Standard.

3	***Departments shall identify and catalogue the key operational services they provide.***	a) Departments **shall** know and record: I. What their key operational services are II. What technologies and services their operational services rely on to remain available and secure III. What other dependencies the operational services have (power, cooling, data, people etc.) IV. The impact of loss of availability of the service
4	***The need for users to access sensitive information or key operational services shall be understood and continually managed.***	a) Users **shall** be given the minimum access to sensitive information or key operational services necessary for their role. b) Access **shall** be removed when individuals leave their role or the organisation. Periodic reviews **should** also take place to ensure appropriate access is maintained.
5	**PROTECT** ***Access to sensitive information and key operational services shall only be provided to identified, authenticated and authorised users or systems.***	a) Access to sensitive information and services **shall** only be provided to authorised, known and individually referenced users or systems. b) Users and systems **shall** always be identified and authenticated prior to being provided access to information or services. Depending on the sensitivity of the information or criticality of the service, you may also need to authenticate and authorise the device being used for access.

6	***Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.***	This section covers four main areas of technology. **a) To protect your enterprise technology, you <u>shall</u>:** I. Track and record all hardware and software assets and their configuration II. Ensure that any infrastructure is not vulnerable to common cyber-attacks. This **should** be through secure configuration and patching, but where this is not possible, then other mitigations (such as logical separation) **shall** be applied. III. Validate that through regular testing for the presence of known vulnerabilities or common configuration errors. IV. Use the UK Public Sector DNS Service to resolve internet DNS queries. V. Ensure that changes to your authoritative DNS entries can only be made by strongly authenticated and authorised administrators. VI. Understand and record the Departmental IP ranges. VII. Where services are outsourced (for example by use of cloud infrastructure or services), you **shall** understand and accurately record which security related responsibilities remain with the Departments and which are the supplier's responsibility. **b) To protect your end user devices, you <u>shall</u>:** I. Identify and account for all end user devices and removable media. II. Manage devices which have access to sensitive information, or key operational services, such that technical policies can be applied and controls can be exerted over software that interacts with sensitive information. III. Be running operating systems and software packages which are patched regularly, and as a minimum in vendor support. IV. Encrypt data at rest where the Department cannot expect physical protection, such as when a mobile device or laptop is taken off-site or on removable media. V. Have the ability to remotely wipe and/or revoke access from an end user device.

		c) To protect email, you <u>shall</u>: I. Support Transport Layer Security Version 1.2 (TLS v1.2) for sending and receiving email securely. II. Have Domain-based Message Authentication Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) records in place for their domains to make email spoofing difficult. III. Implement spam and malware filtering, and enforce DMARC on inbound email. **d) To protect digital services, you <u>shall</u>:** I. Ensure the web application is not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities[3]. II. Ensure the underlying infrastructure is secure, including verifying that the hosting environment is maintained securely and that you have appropriately exercised your responsibilities for securely configuring the infrastructure and platform. III. Protect data in transit using well-configured TLS v1.2. IV. Regularly test for the presence of known vulnerabilities and common configuration errors. You **shall** register for and use the NCSC's Web Check service.
7	***Highly privileged accounts should not be vulnerable to common cyber-attacks.***	a) Users with wide ranging or extensive system privilege **shall** not use their highly privileged accounts for high-risk functions, in particular reading email and web browsing. b) Multi-factor authentication **shall** be used where technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. Multi-factor authentication **shall** be used for access to enterprise level social media accounts. c) Passwords for highly privileged system accounts, social media accounts and infrastructure components **shall** be changed from default values and **shall** not be easy to guess. Passwords which would on their own grant extensive system access, **should** have high complexity.

[3] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

8	**DETECT** ***Departments shall take steps to detect common cyber-attacks.***	a) As a minimum, Departments **shall** capture events that could be combined with common threat intelligence sources e.g. Cyber Security Information Sharing Partnership (CISP) to detect known threats. b) Departments **shall** have a clear definition of what must be protected and why (based upon Standard 1), which in turn influences and directs the monitoring solution to detect events which might indicate a situation the Department wishes to avoid. c) Any monitoring solution **should** evolve with the Department's business and technology changes, as well as changes in threat. d) Attackers attempting to use common cyber-attack techniques **should** not be able to gain access to data or any control of technology services without being detected. e) Digital services that are attractive to cyber criminals for the purposes of fraud **should** implement transactional monitoring techniques from the outset.
9	**RESPOND** ***Departments shall have a defined, planned and tested response to cyber security incidents that impact sensitive information or key operational services.***	a) Departments **shall** develop an incident response and management plan, with clearly defined actions, roles and responsibilities. A copy of all incidents **shall** be recorded regardless of the need to report them. b) Departments **shall** have communication plans in the event of an incident which includes notifying (for example) the relevant supervisory body, senior accountable individuals, the Departmental press office, the National Cyber Security Centre (NCSC), Government Security Group (Cabinet Office), the Information Commissioner's Office (ICO) or law enforcement as applicable (not exhaustive). c) In the event of an incident that involves a personal data breach Departments **shall** comply with any legal obligation to report the breach to the Information Commissioner's Office. Further information on this can be found here.

		d) The incident response and management plan **should** be tested at regular intervals to ensure all parties understand their roles and responsibilities as part of the plan. Post testing findings **should** inform the immediate future technical protection of the system or service, to ensure identified issues cannot arise in the same way again. Systemic vulnerabilities identified **shall** be remediated. e) On discovery of an incident, mitigating measures **shall** be assessed and applied at the earliest opportunity, drawing on expert advice where necessary (e.g. a Cyber Incident Response (CIR) company or NCSC). f) Post incident lessons **shall** be assessed and lessons implemented into future iterations of the incident management plan.
10	**RECOVER** ***Departments shall have well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise.***	a) Departments **shall** identify and test contingency mechanisms to continue to deliver essential services in the event of any failure, forced shutdown, or compromise of any system or service. This may include the preservation of out of band or manual processes for essential services or CNI. b) Restoring the service to normal operation **should** be a well-practised scenario. c) Post incident recovery activities **shall** inform the immediate future technical protection of the system or service, to ensure the same issue cannot arise in the same way again. Systemic vulnerabilities identified **shall** be remediated.