Cabinet Office

HMG Security Policy Framework

Version 1.1 - May 2018

Version History

Document Version	Date Published	Summary Of Changes
1.0	April 2014	N/A
1.1	May 2018	Minor amends – Changes in Data Protection legislation (GDPR).

Foreword

Sir Jeremy Heywood – Cabinet Secretary
Chair of the Official Committee on Security (SO)

As Cabinet Secretary, I have a good overview of the many excellent services the Civil Service is responsible for, and of course the wide range of challenges that we need to manage to deliver them.

The right security, appropriately tailored to take proper account of the very wide range of different jobs we do, assets we handle and environments we work, is a critical pre-requisite for meeting many of these challenges. It ensures we can keep and develop the public's trust that we will handle their information properly, advise Ministers in confidence, and protect the many commercial and financial interests we are responsible for. And of course, it helps maintain national security.

Getting security right has never been more important as the Civil Service continues to modernise and improve our ways of working, and deliver more and more services online. There are longstanding threats and risks to bear in mind; but we must also continue to develop our growing appreciation of global and cyber challenges, critical infrastructure dependencies, together with wider resilience and sustainability issues.

Responsibility for the security of government is delegated down from the Prime Minister and Cabinet to me, as Cabinet Secretary and Chairman of the Official Committee on Security, and then to Heads of Department. It is important therefore to understand our expectations which are set out very clearly in this Security Policy Framework. It should be applied across HMG, but also in respect of assets that are held by third parties in the wider public sector and by our commercial partners.

The Framework incorporates the new Classification Policy launched this month and I am pleased that it makes much throughout of the importance of proper, meaningful engagement of all staff on security matters. No matter how much technology develops people remain our strongest asset. So proper management, good judgment and discretion remain the most effective security protection. The emphasis upon personal responsibility and accountability that underpins the new policy is a key feature of the Framework, and reflects the same obligations that the Civil Service Code places upon us all.

I invite all Boards to act on the introduction of this new Framework and to bring it to the widest attention of colleagues and partners.

SIR JEREMY HEYWOOD

Cabinet Secretary
April 2014

The Security Policy Framework

The Prime Minister is ultimately responsible for the overall security of HMG. They are supported by the Cabinet Secretary, who chairs the Official Committee on Security (SO). Across HMG responsibility for the security of organisations lies with the respective Ministers, Permanent Secretaries and Management Boards.

This Framework describes the Cabinet Secretary and SO's expectations of how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely.

Overarching Principles

There are some principles common to every area of security:

1. Protective security should reflect the UK's widest national security objectives and ensure that HMG's most sensitive assets are robustly protected.

2. Security must enable the business of government and should be framed to support HMG's objectives to work transparently and openly, and to deliver services efficiently and effectively, via digital services wherever appropriate.

3. Risk management is key and should be driven from Board level. Assessments will identify potential threats, vulnerabilities and appropriate controls to reduce the risks to people, information and infrastructure to an acceptable level. This process will take full account of relevant statutory obligations and protections, including data protection legislation, the Freedom of Information Act, the Official Secrets Act, Equality Act, and the Serious Organised Crime and Police Act.

4. Attitudes and behaviours are fundamental to good security. The right security culture, proper expectations and effective training are essential.

5. Policies and processes will be in place for reporting, managing and resolving any security incidents. Where systems have broken down or individuals have acted improperly, the appropriate action will be taken.

Security Outcomes

The Cabinet Secretary and SO expect all HMG organisations (and partners handling HMG information) to meet a range of mandatory security outcomes described below. These outcomes do not specify particular processes but describe what good security will look like. HMG organisations will consult the full range of policy, advice and guidance provided by the Cabinet Office, Centre for the Protection of National Infrastructure, National Cyber Security Centre, and other sources of good practice to shape their business specific approaches, mindful that:

- Government organisations know their own business best, including how local risks should be managed to support operations and services.
- Permanent Secretaries/Heads of Department are accountable to Parliament for the security of their organisations.
- An annual reporting process (the Security Risk Management Overview) will ensure compliance and an appropriate level of commonality across government.

Good Governance

Effective leadership is a critical component of good security and accountability. The Permanent Secretary (or equivalent) will own the organisation's approach to security and ensure that these issues receive the attention and investment required.

Government organisations will have:

a. An appropriate security governance structure to support the Permanent Secretary, that is properly resourced with individuals who have been appropriately trained. These include:

- A Senior Information Risk Owner (SIRO).
- A Departmental Security Officer (DSO) who can manage day-to-day protective security.
- Information Asset Owners (IAOs) across distinct business units.
- Information risk assessment and risk management specialists.

- Other specialists relevant and specific to the organisation's needs.

b. Board-level oversight of security compliance and auditing processes.

c. Arrangements to determine and satisfy themselves that Delivery Partners, service providers and third party suppliers, apply proper security controls too (including List X accreditation for companies handling SECRET assets).

Culture and Awareness

Everyday actions and the management of people, at all levels in the organisation, contribute to good security. A strong security culture with clear personal accountability and a mature understanding of managing risk, responsibility and reputation will allow the business to function most effectively.

Government organisations will have:

a. A security culture that supports business and security priorities and is aligned to HMG's overarching priorities and the organisation's own appreciation of risk.

b. Training which encourages personal responsibility and good security behaviours.

c. Processes, systems and incentives to deliver this.

d. Mechanisms to drive continuous improvement, tackle poor and inappropriate behaviour, enforce sanctions and encourage the sharing of best practice.

Risk Management

All HMG activities attract risk. Risks need to be assessed by government organisations so that they can make informed, practical and effective business enabling decisions.

Government organisations will have:

a. A mature understanding of the security risks throughout the organisation,

where appropriate this will be informed by the National Technical Authorities.

b. A clearly-communicated set of security policies and procedures, which reflect business objectives to support good risk management.

c. Mechanisms and trained specialists to analyse threats, vulnerabilities, and potential impacts which are associated with business activities.

d. Arrangements to determine and apply cost-effective security controls to mitigate the identified risks within agreed appetites.

e. Assurance processes to make sure that mitigations are, and remain, effective.

Information

The security of information is essential to good government and public confidence. To operate effectively, HMG must maintain the confidentiality, integrity and availability of its information.

Government organisations will have:

a. Staff who are well trained to exercise good judgement, take responsibility and be accountable for the information they handle, including all partner information.

b. Mechanisms and processes to ensure assets are properly classified and appropriately protected.

c. Confidence that security controls are effective and that systems and services can protect the information they carry. There will be an overarching programme of information assurance driven by the Board.

Technology and Services

The delivery of efficient public services, including the proper protection of citizen data, requires modern and functional technology. Resilience to cyber threats, compliance with data protection laws and management of national security-related information within these systems will require security to be integral to their design and implementation.

Government organisations will have:

a. Identified if technology and services are Critical National Infrastructure, and risk manage accordingly.
b. Risk-informed security controls which:

- Mitigate applicable threats.
- Are kept current and actively managed.
- Protect against, detect and correct malicious behaviour.
- Ensure that critical technology and services are resilient to disruptive challenges such as cyber attacks, and have the means to recover from these.

Personnel Security

People are an organisation's most important asset, so personnel assurance is fundamental to good security. Government organisations will deliver the appropriate combination of recruitment checks, vetting and on-going personnel security management to be assured, and to remain assured, about their people and to mitigate the risks from well-placed insiders.

Government organisations will have:

a. Joined-up HR and personnel security policies and processes, including recruitment checks (the Baseline Personnel Security Standard (BPSS)) for those with access to HMG assets.

b. Processes to evaluate areas of particular insider risk which require corresponding and proportionate levels of vetting.

c. Robust arrangements for managing the delivery of vetting services, and mechanisms to handle appeals.

d. Effective aftercare arrangements that include regular security appraisals, promote a security conscious culture, and drive staff and line management engagement.

Physical Security

Appropriate physical security measures will ensure a safe and secure working environment for staff that can protect against a wide range of threats (including theft, terrorism or espionage).

Government organisations will have:

a. Processes and plans in place, including those developed from the early stages of building design, to determine the appropriate physical security requirements through planning and risk assessment.

b. Mechanisms to implement internal and external security controls in a layered fashion that deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attack.

c. Substantial controls for controlling access and proximity to the most high risk sites and Critical National Infrastructure assets.

Preparing for and Responding to Security Incidents

Well-tested plans, policies and procedures will reduce organisations' vulnerability to security incidents (especially from the most serious threats of terrorism or cyber attack), but also leaks and other disruptive challenges.

Government organisations will have:

a. Business continuity arrangements aligned to industry standards, to maintain key business services, building resilience and security to facilitate a rapid and effective response to recover from incidents.

b. Processes in place to regularly conduct risk and vulnerability assessments and review resilience planning for critical assets, particularly those identified as Critical National Infrastructure.

c. Counter-terrorism contingency plans in place setting out procedures to be followed in the event of a terrorist threat, including procedures to immediately adjust security requirements around the Government Response Level system.

d. Effective management structures that ensure shared communications between HR and security teams and provide policies and procedures for

detecting, reporting, responding to and handling incidents, including disciplinary measures that are well communicated and understood by staff.

e. Reporting mechanisms to the Cabinet Office Government Security Group, regarding incidents of unauthorised disclosure and breaches of official information, including incidents concerning classified information from foreign governments, agencies or organisations. In addition, such mechanisms should also exist to the Information Commissioner's Office for if and when a serious loss or breach of personal data occurs, in line with data protection legislation.

Policy Priorities

Protective security should always be approached in the round (holistically), but it is helpful to bear in mind specific areas of information, physical and people security. HMG policy across these three areas is set out below:

Information Security

All information that HMG deals with has value. HMG handles the wide variety of information that it generates, collects, processes, stores and exchanges appropriately to ensure: the confidentiality of citizen data and commercial information; good government and the effective and efficient delivery of public services; the proper protection of national security-related information; and that obligations to international partners are met. HMG expects its' partners in the wider public sector, suppliers and other commercial partners who handle information on HMG's behalf to do the same.

HMG operates a Classification Policy to identify and value information according to its sensitivity and to drive the right protections. This comprises three levels: OFFICIAL, SECRET and TOP SECRET for which there are distinct security arrangements. OFFICIAL covers most of the day-to-day business of government, service delivery, commercial activity and policy development.

SECRET and TOP SECRET information will typically require bespoke, sovereign protection, but OFFICIAL information can be managed with good commercial solutions that mitigate the risks faced by any large corporate organisation. In this way government can deliver securely and efficiently, and shape its services to meet the user needs.

The effective management of information is critical to safeguarding it. Government organisations will consider good information management practice as the basis for their information security arrangements.

Technology and Services

HMG will deliver services to the public digitally wherever it can. These services must be designed and delivered securely. A Public Services Network (PSN) offers an infrastructure across the public sector to increase efficiency and reduce overall expenditure. Organisations will utilise appropriate technologies (including mobile

devices) and services (including Cloud) and secure these by default wherever possible. Contracts will specify security requirements clearly.

For new policies or projects that include the use of personal information, an initial assessment on the privacy risks to individuals in the collection, use and disclosure of the information, is made. All ICT systems that manage government information or that are interconnected to them are assessed to identify technical risks. Proportionate assurance processes will provide confidence that these identified risks are being properly managed. This also takes account of risks originating from within the organisations, which could arise from poor behaviours and malicious insiders.

Accountability

HMG organisations are responsible for the information they handle under appropriate governance structures, including at Board level lead. A SIRO is accountable and responsible for information risk across the organisation, supported by IAOs from distinct business units. The SIRO will ensure that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately. HMG continues to remind the public of the importance of protecting their own information online and when accessing government services.

Physical Security

HMG has a wide, diverse estate at home and abroad, including administrative HQs, military bases, Embassies, public offices, and service centres. To ensure: the proper protection of citizen data, commercial confidences, and national security related information; good government and the efficient delivery of public services; and a safe working environment for staff and visitors, a range of physical security controls are required. HMG assets held or managed by third parties must be similarly protected.

The range of physical controls will vary depending upon circumstances and business requirements, and the type of threats (including natural hazards, other disruptive challenges, crime, terrorism, and espionage). Organisations will layer their security, including: perimeter controls and guarding; building design features; limiting, screening or otherwise controlling access; appropriate fittings and office furniture; and the use of separate areas in buildings for particularly sensitive work. Controls should not be onerous but proportionate to ensure the safety and security of staff and visitors.

HMG organisations should also have in place arrangements to adapt and enhance security measures if there is an increase in threats, especially from terrorism. In such circumstances, it may be necessary to limit non-essential access; to increase the frequency of staff and visitor checks and bag searches; and to establish additional

perimeter controls and other guarding activities. Response mechanisms and contingency plans are in place to respond to possible critical security incidents and to enable the continuity of services.

Personnel Security and National Security Vetting

Personnel security controls confirm the identity of individuals (employees and contractors) and provide a level of assurance as to their trustworthiness, integrity and reliability. Whilst HMG personnel security controls cannot provide guarantees, they are sensible and important precautions.

It is HMG's policy that all areas of government and the national infrastructure should include in their recruitment processes certain basic checks. These checks include verification of the applicant's identity, employment history, their right to work in the UK and, if appropriate, checks of any unspent criminal records. Within government these controls are described in the Baseline Personnel Security Standard.

National Security Vetting

National security vetting comprises a range of additional checks and may be applied where policy or a bespoke risk assessment indicates it is proportionate to do so. The risk assessment process takes account of the access an individual may have to sensitive assets (physical, personnel or information) at risk from a wide range of threats. These threats will include: terrorism, espionage, or other actions that could threaten the UK.

There are three different types of national security vetting clearance: Counter-Terrorist Check (CTC), Security Check (SC), and Developed Vetting (DV). Before any such clearance is undertaken the requirements of the Baseline Personnel Security Standard must be met. Whilst the information required and the range and depth of checks undertaken at each level may vary, they are all intended to allow Government departments and agencies, the Armed Forces and police forces to assess whether individuals who are to be employed in sensitive posts or critical functions might represent a security risk either directly or indirectly.

Ongoing Personnel Security Management

The national security vetting process provides an assessment of the vetting subject at the time the process is carried out, but active, ongoing personnel security management is required to ensure that a security clearance maintains its currency. As a minimum, this will involve active consideration of the vetting subject's continuing conduct in respect of security matters; it will also require checks to be repeated at regular intervals.

Any enquiries regarding this publication should be sent to us at GSSmailbox@cabinet-office.x.gsi.gov.uk

You can download this publication from www.gov.uk.