Cabinet Office

Government Security: Roles and Responsibilities

Version 1.0 November 2018

Version History

SPF Version	Document Version	Date Published	Summary Of Changes
1.1	1.0	November 2018	Replaces Roles and Responsibilities Policy (V.4.2) 2011

Contents

POLICY SUMMARY AND CONTEXT

1. The 2016 Transforming Government Security Review recommended the simplification of security governance and accountability. The Transformation programme includes initial development of the Government Security Profession and the recruitment of Security Adviser as part of recruiting and retaining much needed skills to deliver the step-change in security outlined in the Review.

2. As a result of the Transformation programme and of the recruitment of Security Adviser and Chief Security Officers, the Departmental Security Officer (DSO) role will formally end. **Cabinet Office mandates that no new Departmental Security Officers (DSOs) that correspond to Roles and Responsibilities Policy Document (V.4.2)** (and/or listed in those organisations involved in the Clusters)**, are appointed and that those organisations in the Cluster Security Units appoint Security Advisers through fair and open competition.**

3. In addition, **the Senior Information Risk Owner (SIRO) role, unique to government and created in response to HMRC's data loss and the subsequent Data Handling Review, is also no longer mandated by the Cabinet Office in the new structure.** The 2016 Transforming Government Security Review mandated the removal of legacy structures to avoid compliance with outdated standards and processes.

4. The Government Security Roles and Responsibilities policy sets out the foundation upon which good security is built. These include the business area, security and risk management, ensuring security policy and standards are applied more consistently and to improve security professionalism across government. All departments, through their Permanent Secretary as Accounting Officer, retain responsibility for departmental security in the new structure. **The Policy is founded on the principle that security is everyone's responsibility and an integral part of everyone's role.** This enables the organisation to operate flexibly, effectively and securely.

5. It should also be noted that this is an evolving policy, and may be adapted to meet key requirements during the transition to Cluster Security Units.

INTRODUCTION

7. The purpose of this policy is to establish the appropriate protective security roles and responsibilities in departments to ensure an effective risk based approach to security is being taken across the whole business.

8. The policy forms part of the UK Government's internal control and governance arrangements.

9. The policy documents the roles and responsibilities of Departmental Boards, specific Board members, senior Departmental security officials and other key parties required for the collective oversight of security and risk.

10. The policy addresses the changes in relation to the Transforming Government Security Programme and the new roles of the Chief Security Officer and Security Adviser[1] which will replace the Departmental Security Officers.

11. All branches of government must implement effective personnel, physical, technical and cyber security regimes and appropriate levels of security in the face of continuous attempts by hostile and criminal actors to gain unauthorised access or damage the operations or reputation of government and the wider public sector, and to protect against unmanaged impacts on public services. All employees and contracted workers must adhere to the appropriate security standards and common protocols as set by this policy.

[1] For the purposes of this document Senior Security Advisers, Security Advisers and Deputy Security Advisers are referred to as Security Advisers

SECURITY CULTURE

13. A strong security culture is the foundation upon which good security is built. Security is everyone's responsibility and an integral part of their role, enabling the organisation to operate flexibly, effectively and securely. All staff must understand what their specific security and security risk management responsibilities are, depending on their particular role in the organisation.

14. Staff responsibilities can range from complying with basic minimum government security standards and exercising appropriate vigilance against suspicious items or behaviour, to applying the different levels of security controls and protocols described throughout the Security Policy Framework, and/or security industry standards.

15. It is incumbent on all civil servants to promote, implement and adhere to the specific responsibilities placed upon individuals by the Civil Service Code and Management Code, Data Protection legislation and other relevant legislation such as the Official Secrets Act and Computer Misuse Act. This includes compliance with security policies and requirements approved by the Government Security Board or senior accountable officers, such as the relevant Accounting Officer, Chief Security Officer or Security Adviser (SA). These may be incorporated in, or be in addition to department-specific rules or guidance, for example, relating to employee standards of behaviour, or departmental IT acceptable use policies.

16. Staff are responsible for implementing and championing relevant security standards, security-conscious behaviours and good security risk management practices within their areas of work and responsibility.

GOVERNMENT SECURITY ACCOUNTABILITY

17. The Prime Minister and Cabinet are ultimately responsible for the security of Government. Practical responsibility is delegated across HMG to the Cabinet Secretary, respective Ministers, Permanent Secretaries and Management Boards or Executive Teams.

18. HMG works closely with the intelligence agencies and other organisations to keep government safe. In particular, HMG organisations will consult the full range of policy, advice and guidance provided by the Cabinet Office, National Cyber Security Centre (NCSC), Centre for the Protection of National Infrastructure (CPNI), and the UK National Authority for Counter-Eavesdropping (UKNACE), which are the UK National Technical Authorities for cyber, personnel, and physical security, and technical protective security, respectively. Other sources of international standards and good practice also shape business specific approaches. Organisations should remain mindful that:

    a. Government organisations know their own business best, including how local risks should be managed to support operations and services.
    b. Permanent Secretaries/Heads of Department are accountable to Parliament for the security of their organisations.
    c. An annual reporting process will support security performance measurement and an appropriate level of commonality across government, and should be linked to each organisation's internal audit and annual audit, and risk assurance governance and processes.

19. Good governance is crucial to ensure board-level oversight of security compliance and auditing processes including arrangements to determine and satisfy that Delivery Partners, service providers and third party suppliers, apply proper security control (including List X accreditation for companies handling SECRET and above assets), including understanding and managing security issues that arise because of dependencies on external suppliers or through their supply chain.

20. In July 2016 the Permanent Secretary Committee on Security (SO) agreed that the Cabinet Office should produce minimum security standards to improve the quality of security delivery in government. The Cabinet Office Government Security Group (GSG) have issued minimum standards for physical security, personnel security, cyber security and incident management in collaboration with departments, and the National Technical Authorities.

21. The standards define the minimum security measures that departments must implement to meet their SPF obligations, whilst allowing departments flexibility in how the standards are implemented, dependent on their local context.

PRINCIPLES AND APPROACH

The following are key principles for implementing government security:-

22. The organisation's Accounting Officer is formally accountable, under the Security Policy Framework, for ensuring the security of the organisation and its assets;

23. Organising and delivering effective security must be based on a clear understanding of the organisation's assets, for example, people, information, intellectual property or physical assets – and a strong security risk management culture which seeks to identify, manage and mitigate security risks in accordance with the security standards;

24. Responsibility for the identification and management of security risks sits with the relevant Board or Executive Team member who is accountable for the delivery of that area of the department's business.

25. In delivering against these principles, it is expected that the designated Board Member or Accountable Official, working with their Senior Security Adviser, adhere to the principles set out in the minimum security standards to ensure any security incidences and breaches are properly managed, recorded and reported.

SECURITY RESPONSIBILITIES

27. The Security Policy Framework provides the broad framework for the policies, standards, best-practice guidelines and approaches that are required to protect UK government assets (people, information and infrastructure). It focuses on the outcomes that are required to achieve a proportionate and risk-managed approach to security that enables government business to function effectively, safely and securely. However, it may be the case that these responsibilities will combine with other roles and functions within the department. Therefore, departmental or organisational boards or heads of the security function shall at least ensure that the most relevant aspects of the functions are undertaken within the roles outlined, and in a way that is consistent with segregation of duties to ensure the least conflict of interest.

BUSINESS AREA SECURITY RISK MANAGEMENT

29. The most appropriate Board Member, or Executive Director/Directors-General, shall discharge oversight and responsibility for security risk management in their business area.

30. Subject to Departmental needs, they should be supported by:

a. **Senior Security Adviser (SSA)/Security Adviser (SA):** The Security Adviser is responsible for articulating the security needs of their department, overseeing and reporting on the delivery of services to agreed standards, including being the responsible owner for local security policies. They will be acting as an intelligent customer for their department/agency appropriating services from their Cluster Security Unit as necessary. In particular, they should support their Department's security infrastructure and procedures through recognition of the security profession and its functional standards and by securing funding for professional training, qualifications and continuous development. The Security Adviser role is a specific role relating to those organisations involved in the Cluster Security Units.

b. **Risk Owners (RO):** Named senior individuals in business areas who on a day-to-day basis are responsible for the delivery of a function, service, programme or project, and who take operational decisions in direct response to risk, not just limited to security.

c. **Information Asset Owners (IAO):** Named senior individuals responsible for each identified information asset (e.g. database or ICT system) at the appropriate business level within a Department/Agency.

d. **Data Protection Officer (DPO):** An enterprise security leadership role required by data protection legislation. DPOs are responsible for advising accounting officers and senior boards (e.g. ExCo) about the organisation's compliance with data protection law and best practice including explaining residual risk and addressing privacy requirements. To avoid conflicts of interest, this role should not deliver or oversee design or implementation of data protection policies.

e. **Communications Security Officer (ComSO)**: The ComSO is responsible for developing and implementing Communications and Cryptographic policy and procedures within their Department or Agency, or for the organisations in a Cluster, in accordance with HMG policy and Standards as specified and issued by the National Cyber Security Centre, the National Technical Authority for Cryptography.

f. **Crypto-custodian:** If cryptographic material is handled, a Crypto-custodian should be appointed at each location where cryptographic items are held, to follow appropriate policies and standards as set by the ComSO. Where cryptographic items are handled by Cluster Security Units the same processes and standards apply.

g. **Chief Information Security Officer (CISO):** A CISO is a designated individual responsible for the security of information in electronic form. They should advise the Board on how best to exploit technology to deliver the organisation's strategic objectives, and provide strong strategic leadership for the organisation's IT community and its investment in technology. They will be responsible for a departments IT strategy, IT architecture, IT policies and standards, technology assurance and IT professionalism.

h. **Intelligence Handling Coordinator** – Each organisation in receipt of UK Intelligence Community (UKIC) material shall have a designated, expert (Corporate) handling officer whose primary task is to maintain the security of that material by the effective application of intelligence handling policy; this may be an in-house resource or one shared with another organisation(s). The duties of this role are broad and may vary between organisations, and include managing the requirements of readers, SIA Accreditors and Clearance Administrators/Authorities, providing relevant support, advice and guidance on intelligence handling security matters.

31. It is to be noted that the roles described above explain the nature of functions but do not mandate a post for each role.

HMG AND CLUSTER SECURITY

33. The 2016 Transforming Government Security Review recommended to:

   a. Simplify governance and accountability in the centre and in departments
   b. Implement a clustering model for the delivery of security and providing Cluster Security Units (CSU) for Government Departments and agencies
   c. Support these clusters with security shared services

34. The Government Chief Security Officer (GCSO) leads the Government Security Group in Cabinet Office, which brings together strategy, policy development, compliance and the Transforming Government Security Programme (TGSP).

35. **Government Chief Security Officer (GCSO)**

The Government Chief Security Officer is accountable to the Chief Executive of the Civil Service and wider Civil Service Board for setting appropriate government security policies and standards and monitoring performance against them, and is responsible for leading the Government Security Group, overseeing day-to-day operations in support of security across government including response to serious and/or cross-departmental security incidents as well as supporting 'common good' programmes and projects.

36. **Chief Security Officer (CSO)**

The Chief Security Officer is accountable to Departmental Boards within the cluster and the GCSO for the standard of security services delivered by the CSU, and is responsible for leading a cluster security unit, overseeing day-to-day service delivery and ensuring that the Unit has the skills and resources to meet agreed standards and Service Level Agreements as required by the Security Adviser in the departments/agencies.

37. **Cluster Security Unit (CSU)**

The Cluster Security Unit is responsible for the delivery of security services to all government organisations in the cluster in line with agreed standards and Service Level Agreements. This relationship will be underpinned by a Memorandum of Understanding (MOU) to ensure that each party adheres to agreed commitments to uphold the service provision. The CSUs will grow and be designed according to the services being provided and demanded. This will reduce the need for residual security provided in-house by the departments and agencies involved in the CSUs. It is therefore expected that once the CSUs are in full operating capability that the organisation's security services should be delivered by the CSUs.

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