Security Aspects Letters

# Security Aspects Letters

## Purpose

The Ministry of Justice (MoJ) will issue a Security Aspect Letter (SAL) where appropriate.

SALs are generally not required at OFFICIAL but MoJ may issue a SAL where it is optimal to do so or to supersede existing SALs from the previous classification scheme.

This page was last updated on 2018-12-21

## Template

Dear <NAME OR ROLE OF SECURITY DIRECTOR>,

**Subject: Security Aspects Letter**

This Security Aspects Letter ('SAL') establishes the security principles which <ORGANISATION LONG LEGAL NAME, should be highest entity position such as the Group Plc> and/or its affiliates (together "<ORGANISATION SHORTNAME>") shall comply with in producing, handling or storing materials, information or data pertaining to the Ministry of Justice ('Authority').

This letter applies to <ORGANISATION SHORTNAME> and any relevant subcontractor within <ORGANISATION SHORTNAME>'s supply chain as required.

The following sections have been identified as the main areas where guidance is required. If there are any queries, please ask for clarification.

**Purpose**

This SAL issued by the Authority intends to convey the security principles required of <ORGANISATION SHORTNAME> to appropriately and proportionately ensure adequate confidentiality, integrity and availability of Authority data.

The SAL is not a complete and exhaustive list of requirements and conveys the spirit of information security and risk management requirements.

<ORGANISATION SHORTNAME> is required to ensure a comprehensive approach to information risk management through procedural, policy, personnel, physical and technical controls while in possession of Authority information.

**Markings**

This SAL has been developed under the premise that all information assets will be classified OFFICIAL under the [UK Government Security Classifications Policy (GSCP)](https://www.gov.uk/government/publications/government-security-classifications) and that some may carry additional descriptors (for example, COMMERCIAL) to re-enforce handling requirements (such as 'need to know' principles) through the use of the SENSITIVE handling caveat.

All information must be considered OFFICIAL whether it bears a marking or not.

**Handling Instructions**

It should be noted that assigning an appropriate classification to information remains the responsibility of the creator or owner of the asset. Information marked with the SENSITIVE handling caveat may state, or otherwise be accompanied by, additional handling requirements (for example to limit distribution or define additional access controls) which all recipients including the <ORGANISATION SHORTNAME> must comply with.

In general, the Authority expects <ORGANISATION SHORTNAME> to apply the need-to-know principle to information related to Authority systems, and restrict access to such material to those within <ORGANISATION SHORTNAME> (and its supply chain) who genuinely need it to perform their duties. General system information such as system names, IP addresses, high-level designs, etc does not require special handling protections.

**Legacy Material**

Information marked under the previous classification scheme(s) (such as UNCLASSIFIED, PROTECT, RESTRICTED or CONFIDENTIAL) should be effectively considered OFFICIAL unless otherwise stated.

Information marked under previous classification schemes should be reviewed as to whether the information within requires handling caveat markings and/or particular handling guidance before being re-marked as OFFICIAL.

**Data Aggregation**

In aggregation, the impact of a breach of any of these Security Aspects may be higher than the individual records or documents. <ORGANISATION SHORTNAME> should ensure that aggregated or accumulated collections of information assets are protected appropriately.

**Data Offshoring**

<ORGANISATION SHORTNAME> is permitted to Process Authority data (including Personal Data) outside of the United Kingdom subject to the maintenance of adequate information controls and governance, including (not not limited to), the continuation of the protection of rights and freedoms of Data Subjects in relation to their Personal Data, adequate contractual controls and adequate consideration under the <ORGANISATION SHORTNAME> Information Security Management System (ISMS).

<ORGANISATION SHORTNAME> must not routinely transfer or otherwise Process Authority data within an incompatible legal framework to the United Kingdom - more information on this is available on suitable request from the Authority.

*Definitions are as per the Data Protection Act (2018)*

**Policy Compliance**

Effective and appropriately scoped policy controls must be in place to underpin effective information management.

While related information security management certifications recognised by the British Standards Institution (BSI) such as ISO27001:2013, ISO27002:2013 and [Cyber Essentials Plus](https://www.cyberessentials.ncsc.gov.uk/) are preferred, they are not required subject to comparable controls, policies and practices being in place.

A robust ISMS must be in place that ensures information assets are appropriately protected.

A holistic approach to information security must include staff awareness and training through to robust technical and enforced access controls.

**Physical Security**

Physical locations (such as offices and data-centres) must have appropriate physical security characteristics to safeguard information from informational risks.

**Personnel Security**

All personnel with direct or indirect access to, or influence over, information assets must achieve security clearance to at least the [HMG Baseline Personnel Security Standard (BPSS)](https://www.gov.uk/government/publications/government-baseline-personnel-security-standard).

Some roles and sites may require additional levels of clearance. These will be advised by the Authority to <ORGANISATION SHORTNAME> on a case-by-case basis.

All required security clearances must be achieved, and warranted to the Authority, prior to commencement of work by the individual unless otherwise agreed in writing by the Authority.

Full details of Security Clearance requirements are available with the Authority Vetting policy.

**IT Controls**

**Systems**

IT systems must be assessed under <ORGANISATION SHORTNAME> ISMS to ensure an appropriate level of informational risk understanding and where applicable corresponding controls or risk mitigation strategies.

IT technical controls should make all efforts to align to current recognised good practices and be periodically reviewed (no less than 12 month intervals) to understand and re-align controls where appropriate. Best practices include, but are not limited to, encryption methods, multi-factor authentication and software life cycles.

<ORGANISATION SHORTNAME> must ensure system suitability as per the output of the <ORGANISATION SHORTNAME> ISMS prior to the introduction of non-test data.

<ORGANISATION SHORTNAME> must provide information risk management information to the Authority on request so that the Authority may determine whether the assessment made and controls in place are sufficient and robust.

Any remedial activity that may be required by the Authority will be considered under contractual and commercial arrangements however <ORGANISATION SHORTNAME> must acknowledge that systems must be fundamentally fit for purpose and capable of protecting information assets in proportion to their content and value as defined by <ORGANISATION SHORTNAME> and/or the Authority.

**Data transfer protections (data-in-transit)**

All Authority, or Authority related data (such as professional work product pertaining to or on behalf of the Authority), must be protected against negative events (such as interception, misdirection, manipulation or otherwise unintended outcome) while in transit.

The Authority considers application or transport level encryption to be sufficient at OFFICIAL subject to configuration guidance from the UK National Cyber Security Centre (NCSC) having been met.

Some examples of satisfactory approaches include, but are not limited to:

* Email systems meeting the ['Securing government email' guidance](https://www.gov.uk/guidance/securing-government-email)
* Transport Level Encryption (TLS) version 1.2 and above aligned to NCSC recommended configuration(s)
* Internet Protocol Security (IPSec) aligned to NCSC recommendation configuration(s)
* NCSC-approved products or services for data transfer
* Authority-approved products or services for data transfer

<ORGANISATION SHORTNAME> should discuss with the Authority where deviations from NCSC recommendations may be required due to technological limitations.

**SAL revisions**

The Authority reserves the right to issue a revised SAL at any time.

You are requested to acknowledge receipt of this letter and your acceptance of its terms as incorporated into your contract and binding within 14 days.

You are requested to confirm that the details of this SAL have been brought to the attention of the personnel directly responsible for the security of the services provided to, or in support of, the Authority, that they are fully understood, and that the security and information assurance requirements set out in the contract schedules can and will be taken to safeguard the material concerned within 28 days.

You agree to provide a SAL in similar form to all subcontractors, obtain their acknowledgement and provide a copy to the Authority within 28 days.

Yours sincerely,

**Chief Information Security Officer** **Ministry of Justice (UK)**

## Declaration

<ORGANISATION SHORTNAME> will be required to return a declaration.

*Please sign the declaration below and return this letter to the Authority, keeping a copy for your own records. Should you have any queries, please contact the Authority via your point of contact and/or the contact details located within the SAL.*

**Supplier Declaration**

The <ORGANISATION SHORTNAME> hereby confirms that the associated with the requirements described in this Security Aspects Letter have been brought to the attention of the individuals and organisations directly responsible for the provision of the various services. Additionally, that they are fully understood, and that the required security controls can and will be taken to safeguard the material and assets concerned.

For and on behalf of <ORGANISATION SHORTNAME>

………………………………………….. (name)

………………………………………….. (position) [Should be at least Director level]

……………………………………………(date)

Distribution

Internal within Authority:

Action:

* Authority Security & Privacy

Information:

* Director of Authority Service Delivery
* Head of Service Delivery
* Authority Commercial

External:

Action:

* <ORGANISATION SHORTNAME>