Security Policy for Contractors / Consultants / Suppliers

This document specifies the requirements that must be met by contractors, consultants and suppliers in the handling, management, storage and processing of information belonging to MFAT or its partners.

Information Security

1. Information security is the preservation of confidentiality, integrity and availability of MFAT information, and the protection of all official information from unauthorised disclosure or compromise, both classified and unclassified. It may also include the authenticity, accountability, non-repudiation and reliability of MFAT information depending on circumstances.

Objectives

2. MFAT requires the security of its information to be maintained in order to ensure its operational integrity, that all MFAT information is protected from unauthorised disclosure, distribution, compromise and damage, and that the organisation meets its statutory, regulatory and NZ Government policy obligations.

Legislative, Regulatory and Contractual Requirements

3. The management of MFAT and other official information may engage obligations under the following legislation (note that this list is not exhaustive):
   - *Privacy Act 1993*
   - *Public Records Act 2005*
   - *Official Information Act 1982*
   - *Crimes Act 1961*
   - *Summary Offences Act 1981*
   - *State Sector Act 1988*

4. MFAT is required to comply with NZ Government policy on information security and assurance including:
   - *Protective Security Manual*
   - *Security in the Government Sector*
   - *Protective Security Requirements*
   - *New Zealand Information Security Manual*

5. Any individual or organisation accessing, processing, communicating or managing MFAT's information must do so in a manner that is consistent with MFAT's legal, policy and regulatory obligations.

6. Any processing, copying, release, storage or distribution of MFAT information or data outside MFAT's network may only take place with the express written permission of MFAT, prior to any such processing, copying, release, storage or distribution taking place. This clause applies equally to:

- Contractors, consultants and suppliers who are working within MFAT, and utilising MFAT networks, in which case, written permission is required before any information may be released or distributed outside of MFAT networks/premises, and;
- Contractors, consultants and suppliers who are completing work for MFAT on their own networks/premises, in which case, the contract or project documentation will specify the scope of information that may be generated, developed, replicated and/or stored on the contractor, consultant or supplier's network and premises. Written permission is required for any processing, copying, release, storage or distribution of any MFAT information to any other person, party, network or premises not expressly covered within the scope of the project or matter in respect of which the contractor, consultant or supplier has been engaged.

- Where MFAT considers it necessary (having regard to the type of information that will accessible to the contractor, consultant or supplier), arrangements for information handling protocols will form part of an induction between MFAT and the contractor, consultant or supplier and all personnel undertaking work on the project or matter in respect of which the contractor, consultant or supplier has been engaged will be required to attend an MFAT induction briefing on information security. All persons who receive a briefing will be required to sign an acknowledgement that they have received and understood the briefing.

Access to MFAT Information, Information Assets and Information Systems

7. Unless this clause has been expressly waived, anyone required to access MFAT information and/or work in a MFAT building must either hold, or be prepared to apply for, a New Zealand national security clearance. This entails intrusive identity, nationality and criminal record checks. Security clearances obtained through other government departments may be accepted by MFAT. If access is required to information at higher levels of security classification, additional national security vetting checks may be required.
8. Access to MFAT information, assets and systems will only be granted at the minimum level necessary to achieve business purposes.
9. Access to MFAT information, assets and systems will only be granted to specified approved individuals, and any variation to this list of approved personnel must be approved in writing by MFAT Security Division.
10. When the need to access MFAT information, assets and systems ends, all MFAT equipment (e.g. electronic equipment or media, security passes, etc.) and all copies of MFAT information must be returned to MFAT prior to the termination of the engagement.
11. All MFAT information developed, reproduced or stored on any non-MFAT systems must be destroyed and erased (to MFATs satisfaction) at the completion of the project or matter for which the contractor, consultant or supplier was engaged.
12. MFAT monitors the use of its information, information assets and information systems for lawful business purposes.
13. Anyone granted access to MFAT information, information assets and systems must comply with the requirements of MFAT's Code of Conduct, including its ICT Acceptable

Use Policy. Failure to comply with these policies and other relevant instructions may constitute a breach of contract and lead to termination or legal action.

14. Mobile electronic devices (including cellphones, USB sticks, and laptops) are not permitted to be used within MFAT's premises without express approval.

15. Contractor, consultant or supplier personnel may only enter MFAT premises with an appropriate security pass issued by MFAT, and may only enter areas of MFAT premises commensurate with their function and, where specified, escorted by MFAT staff.

16. Any MFAT information released to contractors, consultants or suppliers for storage or processing outside of the MFAT environment must be stored securely, as specified by MFAT's Security Division.

Information Security Management System Controls

17. Written pre-approval must be granted before any MFAT information may be stored, processed or reproduced on any network, system or device not owned by MFAT, as specified in paragraph 6.

18. Should any information be held within the contractor's, consultant's or supplier's network (as controlled by paragraphs 6, 17 and **Error! Reference source not found.**), the contractor, consultant or supplier must:

    - have a security incident reporting process in place to a standard and design acceptable to MFAT to ensure that any incidents involving MFAT information are immediately reported to MFAT;
    - agree to undertake any remedial action required by MFAT and ensure that this is implemented in an auditable way; and
    - agree to permit and facilitate audits of all aspects of their information security management system by MFAT and to address any findings of such audits in order to preserve the security of information to MFAT's standards and requirements.

19. A contractor, consultant or supplier holding MFAT data on MFAT's behalf must have in place processes to ensure that critical MFAT information held by them can be promptly and efficiently recovered following an emergency.

Information Breaches

20. If a breach of these clauses is identified (including, but not limited to, permitting, facilitating or allowing an unauthorised release of MFAT information), resulting in the compromise of any MFAT information, and the contractor, consultant or supplier (or any of their personnel or subcontractors) is found to be responsible for that breach, the contractor, consultant or supplier will be held liable for the costs of any associated incident investigation, rework, redesign or any other remedial measure, which is required to rectify or mitigate the outcomes of that breach.