Acceptable use policy

Information Services Division

Cataloguing data

This publication (and any material sourced from it) should be attributed as: Information Services Division, *Acceptable use policy*, Department of Agriculture, Canberra, September. CC BY 4.0.

This publication is available at mylink.agdaff.gov.au/Pages/TBC

Department of Agriculture
GPO Box 858 Canberra ACT 2601
Telephone 1800 900 090
Web agriculture.gov.au

Contents

1 About

1.1 Scope

This policy covers all information and communications technology (ICT) services, including the use of networked computers, remote access, email, Internet access, telephones, or mobile devices. This policy forms part of a tiered system of policies, standards and guidelines, as defined in the Information Security Management Framework (ISMF). It replaces any earlier departmental policies concerning ICT acceptable use.

This policy applies to all Department of Agriculture employees (including contractors and sub-contractors) who use departmental equipment, devices, or services as part of their work. Any questions about the application of this policy should be raised with the department's Information Technology Security Adviser (Director, Information Security).

1.2 Objectives

The objective of this policy is to protect the department from actual or potential damage to its business interests, reputation, systems, and information. This is achieved by setting out guidelines and requirements for acceptable use for all services and technology.

Inappropriate use of ICT services has the potential to expose the department's systems to various risks. Transactions or posts to the Internet (or other networks) can be associated with the department and as such may pose a risk to its reputation. For individuals, inappropriate use of ICT services may be investigated as a potential breach of the APS Code of Conduct or constitute fraudulent and/or criminal behaviour.

2 Policy for acceptable use

2.1 Appropriate use

The use of computers, Internet access, telephones, and other equipment and services should support employees in their role and the delivery of business outcomes.

This includes, but is not limited to:

- communicating and providing service to the public, stakeholders, other agencies, and personnel for work-related purposes
- conducting the business of their team
- gathering information relevant to their duties
- gathering information to expand their expertise.

Users of the department's systems must ensure that their usage does not interfere with normal business operations or compromise the department.

The Australian Public Service Commission (APSC) offers some guidance on reasonable personal use of services (including telephone calls, email, and Internet). Guidance on the use of social media is also available on mylink and the APSC website.

The use of business assets or resources for lengthy non-work use, such as for study assignments or community work, is not permitted unless prior approval is obtained from the relevant manager. Departmental assets must not be used in connection with outside employment, including volunteer work or any other income generating activity, unless specifically authorised by the Chief Information Officer.

2.2 Inappropriate Use

Inappropriate use includes, but is not limited to:

- committing identity theft by using another person's name, password, or account to communicate or access the network or Internet—this includes attempting to obtain another user's passphrase or security token;
- running a business outside the department;
- connecting or storing departmental data on personal media or personal devices;
- distributing sensitive or classified departmental or client materials to another party, the public or the Internet—this includes divulging private information (including full name, birthdate, home address, or telephone number) about yourself or other personnel, or sharing information relating to departmental operations and/or transactions
- excessive personal use of departmental resources—this covers any personal use which interferes with business needs or exceeding data allocations. More information about acceptable personal use for mobile devices is available on the Mobile Device Policy Frequently Asked Questions

- searching for, attempting to access, or not otherwise avoiding known sources of objectionable material
- encouraging, enticing or otherwise pressuring associates to search for, attempt to access, or not otherwise avoid known sources of objectionable material
- using, sending, receiving, storing, or otherwise being in possession of objectionable material
- threatening or damaging the network—this includes introducing malware or corrupted data or other attempts to compromise the integrity of the department's network
- using departmental equipment or services to circumvent technical controls, including attempting to access, gain unauthorised access, or scan for vulnerabilities to the department's network or that of any other organisation. Only staff specifically authorised by the Information Services Division (ISD) may carry out vulnerability testing for security audit purposes.

Objectionable material is defined as any material containing content which is illegal, offensive, abusive, threatening, menacing, vulgar or obscene, suggestive, harassing, belligerent, or defamatory. This includes material containing misleading, inaccurate, inappropriate, or controversial content that would likely cause offence.

2.3 Authorisation

All departmental employees need prior authorisation from ISD to:

- make changes to the configuration of installed hardware or software
- download, transfer, or install software, software updates, or software patches for workstations, servers, network devices, or portable devices. ISD is responsible for monitoring issues and providing timely software updates or software patches for any approved software in current use
- connect any workstation, server, network device, or portable device to departmental systems
- connect externally (remote access) into departmental systems. Any remote access must only use approved methods and technology services provided for that purpose. Further restrictions may be placed on the period or purpose for which remote access is/authorised.

No software will be approved without first being evaluated by ISD and having licensing arranged. This includes demonstration software, open-source software, add-on utilities, shareware, and automatic update capabilities. The evaluation process will include analysis for malware functionality and fitness for purpose.

2.4 Monitoring

The department has the right to monitor, investigate and examine all activity conducted through its network or equipment. ISD will audit workstations, servers, network devices, and portable devices on a regular basis to ensure compliance.

The department also has the right to filter or otherwise restrict or block emails, file transfers, or access to specific Internet sites or facilities. Blocked or failed attempts to access these services may also be logged.

Authorised ISD employees may review files and intercept communications for network protection duties. This includes, but is not limited to, maintaining system integrity and ensuring employees are using the system in accordance to departmental policy.

When any computer equipment is connected to the department's network, ICT technical employees are authorised to monitor or access the equipment to rectify situations that threaten the integrity of the department's network, servers, or systems, provided that use of accessed files is limited solely to maintaining or safeguarding departmental systems.

The department may disclose documents, activity logs, email text, and images to regulators, the courts, law enforcement, and other third parties, including internal stakeholders such as Conduct and Performance, Fraud and Corruption and Security, without personal consent.

2.5 Personal responsibility

To protect the information security and business interests of the department, a number of responsibilities need to be clearly understood and properly followed.

All departmental employees are responsible for:

- ensuring the information and data they are entrusted with (including data that has been transferred to portable devices or media) remains confidential and secure as required
- keeping any assigned (or personalised) passphrases and security tokens secure and confidential
- complying with the data or usage limits that apply to their departmental portable electronic devices. Any personal use considered to interfere with business needs and/or exceed these limits may be subject to further enquiry or investigation
- applying due care when introducing or otherwise receiving, copying, or disseminating data onto departmental systems. All employees should avoid introducing malware or spreading any threat or risk that has already been introduced
- applying due care when distributing or sending out data. All employees should take appropriate steps to ensure that the data is malware free before releasing any data, particularly if that same data is to be published for a wide audience
- applying due care when copying or transmitting data. All employees should take appropriate steps to ensure compliance with relevant legislations and regulations. All materials controlled by intellectual property rights (copyright, trademark, or patents) must acknowledge of the holder of those rights. Some materials may have further restrictions on the right to copy or distribute those materials or may require permission from the owner or copyright holder
- caring and safekeeping the hardware and software and attached equipment (peripherals) allocated to them.

2.6 Limitations of service

The department accepts no liability for any direct and/or indirect damages. This includes, but is not limited to, consequential loss, loss of profit and/or loss of opportunity arising from the user's unauthorised or personal use of departmental systems or services.

Users of the department's ICT are responsible for any non-authorised content they disseminate. The department is not responsible for any third-party claim, demand, or damage arising out of the unauthorised use its systems or services.

The department may suspend access at any time without prior notice, for technical reasons, policy violations, or other concerns.

2.7 Data ownership

Data present on departmental systems (or devices), including all documents, messages, database content, or other data file type, are by default the property of the department. Users of departmental ICT systems should ensure that they do not rely on the department to store personal records. The department does not guarantee access to records stored on departmental systems for former employees or former users of the system.

Any departmental data, including but not limited to all documents and files (and any copyright, trademarks, confidential information, know how, databases, and inventions contained in them), remain the property of the department.

No departmental employee should have any absolute expectation of privacy regarding any data they have received, introduced or otherwise stored on the department's systems.

All data held on departmental equipment is to be accessible (at least to system administrators) and subject to all departmental acceptable use and security policies.

Some data held on the department's systems may originate from other agencies or organisations. Approval from the original agency must be sought before disseminating the information outside the department.

3 Compliance

Though each individual is responsible for their own actions, management is responsible for ensuring that their employees, contractors, and other authorised users are aware of their responsibilities under this policy.

Any individual aware of non-compliance with this policy should immediately report the matter to their supervisor or the Director of Information Security. Any potential fraud related to non-compliance with this policy should also be immediately reported to the Fraud & Corruption team (FraudandCorruption@agriculture.gov.au).

The department's IT Security team manages compliance for this policy and may refer non-compliance to other areas of the department for further action as appropriate. Any non-compliance with this policy may result in the matter being investigated—this may be as a Code of Conduct, fraud or security investigation. If proven, the responsible individual may be subject to employment sanctions or criminal investigation.

4 More Information

For more information, contact the IT Security team (ITSecurityOperations@agriculture.gov.au) or visit the IT Security mylink pages.

More information about your rights and responsibilities as an APS employee is also available on the APSC website.