WAIS Information and Communications Technology Management Policy

Owner: Finance and Operations Manager

Version: 3.0

Approved by: Executive Director

Next review date: October 2018

Next review date: October 2016

WESTERN AUSTRALIAN INSTITUTE *of* SPORT

CONTENTS

1. Purpose

To define Information and Communications Technology (ICT) management guidelines to preserve the integrity and security of WAIS ICT systems and their data.

2. Scope

This policy outlines the principles and methodology utilised by WAIS in conjunction with contracted ICT service providers.

Corporate ICT assets include corporate information systems, software, data, and computing assets, which include but are not limited to computers, computer networks, printers, tablets, telephones and other related units of equipment.

3. Standards

3.1 WAIS will define, maintain and monitor user access rights to the WAIS ICT network.

3.2 Access to the WAIS ICT network will be controlled through each user having defined access rights and a password whose parameters and complexity will meet ISO/IEC 27002.

3.3 WAIS will define and maintain a disaster recovery and business continuity plan and ensure systems and operations are in place to implement the plan.

3.4 All external ICT service provision will be under a defined and managed contract that complies with this policy.

4. User Access Control

WAIS users are provided with a user account allowing access to the WAIS network from all locations at any time. The ICT service providers, as the WAIS ID providers, strictly monitor access to the WAIS network and any irregular and illegal attempts to logon to the network by non-WAIS users is promptly detected and reported to the WAIS Finance and Operations Manager.

Security of the WAIS IT network, systems and information is to be maximised by:

4.1 ensuring authorised users are granted only the level of access required to effectively perform their official role and functions;

4.2 ensuring users are advised against attempting to gain, and systems are in place to prevent them gaining, a level of access beyond that officially authorised;

4.3 maintaining records of all security and access privilege requests, authorisations, changes and removals in relation to the IT network, systems and information for audit purposes and security review;

4.4 restricting third party, including vendors, access to the appropriate level required for effective support purposes ensuring approval by WAIS and ongoing monitoring of third party access;

4.5 restricting and controlling administrator rights to IT devices, with requests for access, or assistance to access, requiring approval from WAIS Finance and Operations Manager;

4.6 review the list of active user accounts bi-annually (June and December). User access and privileges for all systems is to be reviewed to ensure that former staff do not have access to the WAIS ICT systems.

4.7 Disabling dormant accounts by default, during monthly reviews of accounts; and an account being re-enabled only following formal approval.

5. Password Management

Unauthorised or improper access to the WAIS IT network, online applications and systems can facilitate cyber-attacks, enable improper disclosure of appropriately confidential information, and result in the malicious corruption or loss of important and possibly irreplaceable official information. The use of passwords is mandatory for all account users so as to gain access to the WAIS IT network, systems and information.

Security of the WAIS IT network, systems and information is to be maximised by:

5.1 assigning a unique user account name and password to identify, authenticate and authorise approved individual access;
5.2 expiring passwords that have not been changed for 60 days;
5.3 not allowing the reuse of recent passwords;
5.4 passwords meeting best practice standards in terms of length and complexity; and
5.5 auditing, verifying and tracking access requests.

6. Internet and email usage

Access to the internet and email is an essential means of communication and enterprise for any organisation, and WAIS recognises its staff conduct regular dealings in an online environment. This environment is constantly and rapidly changing and there is increasing use of social and streaming media for mass communication, making the internet an indispensable tool in effective corporate communications.

It is therefore the policy of WAIS that:

6.1 all WAIS staff are to have internet and email access;
6.2 staff are trusted to adhere to policy and procedures and to exercise good judgment with respect to their online behaviour;
6.3 email should not be used for highly sensitive or confidential information, unless appropriate actions are taken to secure the contents against disclosure, alteration and forgery;
6.4 email must contain a standard approved footer;
6.5 personal use is allowed only if it does not interfere with formal duties and if all relevant policies, procedures and guidelines are followed (examples of permitted personal use include online banking, paying a parking fine, browsing or shopping during a lunch or coffee break);
6.6 WAIS has both the right and the obligation to monitor and electronically record internet usage by staff; and
6.7 any staff member suspected to be contravening the IT Acceptable Use policy will be may have their access restricted, and could face disciplinary procedures as a result.

7. Security and Compliance

WAIS provides a secure network environment for the safe and reliable storage of documents and files. All data files are considered official documents that are subject to the same laws as any other form of correspondence. Files created may be subject to statutory record keeping requirements and can be subpoenaed during legal processes or for annual statutory audit purposes.

Monitoring access, Computer surveillance of ICT resources and other security and control measures will be undertaken by the ICT service providers with the consent of WAIS are to ensure compliance to this Policy. Should the ICT service providers capture an irregular attempt to access or an irregular access to the WAIS operating system, the ICT service providers are to report these attempts to the WAIS Finance and Operations Manager immediately.

To maximise security and compliance:

7.1 all documents and files are to be stored on the WAIS servers;
7.2 all WAIS users are required to read and acknowledge the WAIS IT Acceptable Use Policy before system access is granted;
7.3 all WAIS users are required to accept the WAIS Network disclaimer when logging on to WAIS IT resources;
7.4 WAIS will monitor the levels of demand of the technology, and use this information in planning for future needs;
7.5 the ICT service providers shall keep required details of WAIS users who logon to WAIS network resources;

8. System Development and Change Management

In-house developed ICT systems are the responsibility of the WAIS staff member that created them, as the application custodian they are:

8.1 to document the development of the system;
8.2 to document changes to the system;
8.3 responsible for the ongoing maintenance of this system; and
8.4 responsible for support of the system.

WAIS will contract any other system development, installation, update and maintenance to third parties. Changes to these systems are managed by the WAIS Finance and Operations Manager, as custodian of the WAIS network environment will approve changes, maintenance and updates. The contracted third parties and WAIS employees require authorisation from the WAIS Finance Manager before proceeding with changes to any systems and applications.

Any major changes to systems and applications are to be tested by the contracted third parties or the WAIS Finance and Operations Manager before they run live on the WAIS servers for all users to use.

9. Support

Bekkers is the primary support provider for WAIS Users.

10. Policy Implementation

10.1 Creation of new user accounts

New user accounts are to be obtained by submission of a new user request to the IT provider, specifying applicant details, the level of access sought and the endorsement of a nominated WAIS representative. To request a new user be created and appropriately authorised person from WAIS will lodge a service ticket with Bekkers specifying full user details, the systems that the user will require access too, and the level of access required.

On the completion of the new user request, access to the IT network, systems and information is authorised by assignment of a unique user account name to the approved user and their designation of a confidential password. Users will be prompted to acknowledge the IT Acceptable Use Policy as part of the Windows login process.

New users may only be requested by the;

10.1.1 Administration Manager

10.1.2 Finance and Operations Manager

10.1.3 Executive Director

Or their delegates. Access to executive areas may only be granted by the Executive Director.

10.2 Termination of existing user accounts

All accounts that are inactive for a period greater than 1 month shall be automatically suspended.

The It Provider shall provide notification to the Finance and Operations Manager of accounts that have become inactive and have been suspended.

The WAIS Finance and Operations Manager or Administration Manger shall provide formal notification to the IT Provider of accounts to be terminated when staff permanently leave the organisation.

10.3 Setting User Passwords

A preliminary user password is assigned to a new user by the IT Provider to enable initial access to the IT network. The preliminary password must be changed immediately at first login to a confidential password to allow access to the IT Network.

All user account passwords will automatically expire after 60 days unless the password is reset by the user or, on request, by the IT Provider. Requests from users to change their user account password are to be follow the Password Reset Procedure on receipt of the change password request. Users will be notified to change their password before the expiry date when logging onto the network.

When a user incorrectly types a password more than 3 times when accessing the WAIS operating system, the user account will be temporarily locked out for security reasons

All passwords should:

10.1.1 include a minimum of 8 characters;
10.1.2 be a combination of alpha and numeric characters;
10.1.3 not contain the user's 'user account name' or full name;
10.1.4 not include consecutive words or numbers; and
10.1.5 not include (well known) nicknames, pet names or similar terms.

Note:

- Individual application systems may have a policy of locking the account and require reset by the application owner or vendor, for example Performax.
- Individual application systems may require a response to a security question which will forward the password to an approved email address.
- Staff members are strictly prohibited from disclosing their passwords as this could compromise the security of the IT network, systems and information.

10.4 Access to Shared network resources

Requests to access WAIS network resources by submission of an Access Request to the IT provider, specifying applicant details, the level of access sought and the endorsement of a nominated WAIS representative. The IT Provider will follow the Access Request Procedure on receipt of the request.

10.5 Email Disclaimer

All email messages must contain a standard footer (signature file) that incorporates the sender's name, email address, position, organisation, organisation email address, phone number and a disclaimer stating:

'This email and any files transmitted with it are confidential and may contain privileged or copyright information. If you are not the intended recipient, you must not copy, distribute or use this email or the information contained in it for any purposes other than to notify us. If you have received this message in error, please notify the sender immediately, and delete this email from your system.'

10.6 Breaches

Breaches of this policy will result in a user's account being disabled, the password reset to preclude access, and the WAIS Finance and Operations Manager being notified directly. Breaches of this Policy will be treated in the same manner as the 'Process for Investigating Complaints' as defined in the 'WAIS Staff Code of Conduct'.

Staff found to be violating the Criminal Code in their use of the IT resources must accept personal liability for prosecution.