ICT Acceptable Use Standard

Document Information

Attribute	Information
Document Title	ICT Acceptable Use Standard
Document No	SS-STD-ICT-018
Revision Status	03
Author	Leon du Preez
Publication Date	November 2014

Document Approvals

Action	Role	Signature	Date
Approval By	Chief Information Officer Arthur Madonsela		11/11/2015
Approval By	Manager: ICT Infrastructure and Operations Leon du Preez		23/10/2015
Approval By	Manager: ICT Risk and Compliance Justice Mampuru		04/11/2015
Approval By	Manager: Enterprise and Architecture Darryl Rondganger		23/10/2015

Table of Contents

1. DOCUMENT CHANGE HISTORY

PUBLICATION DATE	AUTHOR	REVISION NO.	CHANGE DESCRIPTION
November 2011	Carl Grundling	00	New
March 2013	Carl Grundling	01	General revision of terms
November 2014	Leon du Preez	02	Reviewed stakeholders and review period
August 2015	Leon du Preez	03	Reviewed content

STANDARD TITLE

ICT Acceptable Use Standard.

2. PURPOSE

The purpose of this standard is to protect the image and reputation of the CSIR, as well as to promote the integrity, availability, and confidentiality of the CSIR's systems, network and data contained therein. It informs the user of the prevailing rules and prohibitions that define and govern acceptable use of such systems and facilities, and outlines the possible results of violation of this standard.

CSIR's Information and Communication Technology ("ICT") comprises the vast and growing array of computing and electronic data communications facilities and services, utilised daily to create, access, examine, store, and distribute material in multiple media and formats. ICT plays an integral part in the fulfilment of CSIR Research, Development and Implementation functions. Users of CSIR's ICT resources have a responsibility not to abuse these resources and to respect the rights of the members of the community as well as the CSIR itself. The CSIR Acceptable Use Standard (the "AUS") provides boundaries for the appropriate use of CSIR's ICT resources as well as for the CSIR's access to information about and oversight of these resources.

3. SCOPE

This standard applies to all employees, contractors, consultants, guests, temporary workers, and all personnel affiliated with third parties doing work with CSIR. This standard applies to all ICT systems and services that is owned or leased by the CSIR.

This standard defines the boundaries for the "acceptable use" of the CSIR's resources, including software, hardware devices, and network systems. Hardware devices, software programs and network systems purchased and provided by the CSIR are to be used only for the creating, researching, and processing CSIR-related materials. By using the CSIR's hardware, software and network systems the employee (user) assume personal responsibility for their appropriate use and agree to comply with this standard, other applicable CSIR policies, as well as laws and regulations.

All of the following are included whether they are owned by, leased by or in the possession of the CSIR:

- All computer-related equipment, including desktop personal computers, laptops, tablets, smartphones, wireless computing devices, telecommunication equipment, networks, databases, printers, servers, internet devices, storage devices,shared computers and all networks and hardware to which the equipment are connected.
- All software including purchased or licensed business software applications, organisational-written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on organisationally-owned equipment.
- All intellectual property and other data stored on organisational equipment.

4. STANDARD

4.1 General use and Ownership

4.1.1 Organisational confidential information may not be shared outside of the organisation, without authorization, at any time.

4.1.2 The CSIR does not guarantee the confidentiality of any private information stored on the CSIR ICT Infrastructure.

4.1.3 Each user assumes responsibility for exercising good judgement regarding the reasonable personal use of CSIR ICT infrastructure, such as the Internet, storage, streaming and/or downloading of data, etc. Use of the Internet for private purposes therefore occurs responsibly and reasonably, with each user recognising that such use may constitute fruitless and wasteful expenditure which in turn constitutes misconduct. If there is any uncertainty in this regard, users should consult their OU/Unit manager or Business Services Manager.

4.1.4 For security or network maintenance purposes, the CSIR reserves the right to audit ICT systems and services by authorised ICT Service Centre personnel at any time.

4.1.5 ICT may during within course and scope of their duties need to disable the network access of a host if such host is disrupting or threatening to disrupt production services.

4.1.6 The following policy considerations apply to the use of Social Media:

- Be responsible in what one writes;
- Remember to protect CSIR confidential & proprietary information;
- Respect copyrights;
- Authenticity;
- Consider your audience;
- Exercise good judgement;
- Understand the concept of community;
- Refrain from making views on behalf of CSIR; and
- Refer any social media enquiries about CSIR to communications department.

4.2 Security and Proprietary Information

4.2.1 Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the course and scope of such employee's work. Disclosing data to unauthorised parties.

4.2.2 Passwords are kept secure and are not shared. Every user assumes responsibility for the security of his/her passwords and accounts. Shared passwords are appropriately managed to minimise risks.

4.2.3 All PCs, laptops and workstations are secured with a password-protected screen saver with the automatic activation feature activated or by logging-off when the device is left unattended.

4.2.4 Postings by employees from a CSIR e-mail address to newsgroups contain a disclaimer clearly stating that the opinions expressed are strictly their own and not necessarily those of the CSIR.

4.2.5 All hosts used by the employee that are connected to the CSIR's Internet/Intranet/Extranet (or used in an 'off-line' state) are continually executing approved virus-scanning software with a current virus database.

4.2.6 Each user should use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses.

4.2.7 Each user assumes responsibility to ensure that visitors who bring their own removable storage devices onto the CSIR campus are supervised at all times whilst the device is connected to CSIR equipment.

4.2.8 Care is taken to ensure that any data storage device with sensitive and/or confidential information is kept secure at all times.

4.2.9 Recognising that the CSIR Bulletin Board runs in the CSIR network and falls under CSIR management, thus rendering the CSIR potentially liable for its contents, it may be used for the dissemination of personal information, such as advertisements, requests etc. The Bulletin Board is not used for chain letters or petitions that may be considered abusive, discriminatory, racist, provocative or offensive in any manner, be it political, religious, social or otherwise. The use of the Bulletin Board remains subject to the rules governing individual rights and respect and non-compliance with this document comprises a breach of the CSIR ICT Policy.

4.2.10 Whenever possible, only connect to wireless networks that require a network security key or have some other form of security, such as a certificate. The information sent over these networks is encrypted, which can help protect your computer from unauthorized access.

4.2.11 Before connecting to a network provided by a wireless Internet service provider (ISP), such as a public network in a coffee shop or airport, read the privacy statement carefully and make sure that you understand which files, if any, are saved to your computer and what type of information the network provider collects from your computer.

4.2.12 Do not leave your laptop unattended unless it is physically secure. Secure your laptop when you are not in your office. Lock your door and/or secure your laptop to the desk with a laptop cable. If you take your laptop home, be sure to keep it in a secure location. Do not leave your laptop in your car.

4.3 Unacceptable Use

The following activities are prohibited:

4.3.1 The transmission, storage or distribution of any material or content where such action would violate any South African or other applicable laws prohibiting child pornography; obscenity; discrimination (including racial, gender or religious slurs) and hate speech; or speech designed to incite violence or hatred, or threats to cause bodily harm.

4.3.2 The transmission, storage or distribution of any material or content where such action is intended to defame, abuse, stalk, harass or physically threaten any individual in the Republic or beyond its borders; including any attempt to link to, post, transmit or otherwise distribute any inappropriate or defamatory material.

4.3.3 The transmission, storage and distribution of any material or content where such action violates any intellectual property laws including laws concerning local and international copyright, trademarks and trade secrets.

4.3.4 Any effort to use the CSIR's ICT systems and services in a way that circumvents or would circumvent the user authentication or security of any host, network or account ("cracking" or "hacking"). In instances where this is a requirement, ICT Service Centre should be notified of the intention via the OU/Unit manager.

4.3.5 Any attempt to use the CSIR's ICT systems and services in a way that breaches or would breach the security of another user's account or that gains or would gain access to any other person's computer, software, or data or otherwise threaten another person's privacy, without the knowledge and consent of such person.

4.3.6 Any activity which threatens to disrupt the CSIR's systems and services through "denial of service attacks"; flooding of a network, or overloading a service or any unauthorised probes ("scanning" or "nuking") of other networks.

4.3.7 Any activity which in any way threatens the security of ICT systems and services by knowingly posting, transmitting, linking to or otherwise distributing any information or software which contains a virus, trojan horse, worm, lock, mail bomb, or other harmful, destructive or disruptive component.

4.3.8 Any unsolicited mass mailing activity including direct marketing; spam and chain letters for commercial or other purposes, without the prior consent of the recipients of those e-mails.

4.3.9 Unauthorised use, or forging, of e-mail header information.

4.3.10 Creating or forwarding "chain letters" or other "pyramid" schemes of any type.

4.3.11 The installation on any computing device to the CSIR's network without prior approval from ICT Service Centre is strictly prohibited. This includes devices such as PC's, laptops, servers, routers, mobile devices, and switches. This excludes the provisioning of guest network access to visitors and their specific computing devices via the CSIR Guest Network for Internet Access initiative.

4.3.12 The use of any portable storage devices to store sensitive, confidential or personally identifiable information without prior authorisation by his/her manager.

4.3.13 The storing of any CSIR sensitive or confidential information on social networking sites such as Flicker, Facebook, MXIT, EverNote, and others.

4.4 ENFORCEMENT

4.4.1 The CSIR reserves the right to audit networks and systems on a periodic basis to ensure compliance with this standard. The Regulation of Interception of Communications and provision of communication-related information Act (RICA) no 70 of 2002, came to effect in 2005. This act requires a written consent from each employee to agree to the interception of any communication and related information (specifically, but not limited to, communication by means of telephone/modem, telefax, Internet or e-mail).

4.4.2 Any employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.

4.4.3 All users must report all suspected cases of violation to his/her appropriate Business Services Manager as well as to the Chief Information Officer.

4.4.4 The Manager: ICT Risk and Compliance will collect the facts (after approval from the Group Executive: Shared Services, of the case and identify the offender. If, in the opinion of the Group Executive: Shared Services, the alleged violation is of a serious nature, the relevant HR Manager will be contacted for further action.

Executive: Shared Services, the alleged violation is of a serious nature, the relevant HR Manager will be contacted for further action.

5 OWNERSHIP AND RESPONSIBILITIES

5.1 Owner

Chief Information Officer.

5.2 Responsibilities

The Chief Information Officer retains all levels of authority for ICT Risk and Compliance.

The Manager: ICT Risk and Compliance is the owner of the documented standard and has the responsibility to ensure that it is followed, regularly reviewed and updated.

6 RECORDS

Description	Location	Responsibility	Retention Time	Disposal Method
ICT Acceptable Use Standard	ICT Website	Chief Information Officer.	Indefinitely	Normal waste
ICT Policy	ICT Website	Chief Information Officer.	Indefinitely	Normal waste
ICT Investigations and Surveillance Procedure	ICT Website	Chief Information Officer.	Indefinitely	Normal waste

7. Requirement for update:

Update every 3 years or as and when required.