Information & Communications Technology Acceptable Use Policy For Staff

RESTRICTED

Version: 1.6

Effective Date
1 Aug 2018

Document Control

Revision History

Version	Date	Description	Author
1.0	23 Mar 2010	Initial Release. Replaces Security Policy Governing the Use of Computer Resources at the Singapore Polytechnic.	EMC Consultant
1.1	1 Nov 2011	Change of password policy to meet password complexity requirement.	Anthony Lau
1.2	1 July 2012	Added section on Privacy.	Anthony Lau
1.3	1 Aug 2014	Updated to align with change of SP ICT Security Policy & Standard.	Deloitte Consultant
1.4	1 Aug 2015	Updated unclassified data definition for clarity and editorial changes.	Jason Tseng
1.5	1 Sep 2016	Editorial changes. Updated security awareness training to annually. Privacy section updated for IM8 alignment.	Jason Tseng
1.6	28 Nov 2017	Logo and editorial changes. Aligned information classification with Greenbook. Changed DITSO to IT Chairman for clarity. Added that inactive accounts will be disabled after 90 days. Added PCEO approval required for access to user data in SP assets. Added compliance audit as required in IM8. Added controls on use of portable storage devices. Updated traveling requirements with ICT assets. Updated SP Information Classification	Jason Tseng

Reviewers

Name	Role	Status
Chairman & Members	ICT Working Committee	Endorsed

Approvals

Name	Title	Date
Chairman & Members	ICT Steering Committee	1 Aug 2018

Distribution

A soft copy of this document is available in Staff Portal and accessible to all SP staff. External parties who require access SP ICT resources, may be given a copy to acknowledge compliance to the policy.

Table of Contents

1. Introduction

As an employee of Singapore Polytechnic, you will make use of the Polytechnic's ICT Assets such as information, computers, networks and software in your day-to-day activities. It is important that these important resources provide the service to you and to others for which they were intended.

An important part of the proper operation of these ICT Assets is security. Trojans, viruses, worms and spyware can wreak havoc on these assets, so the Polytechnic has taken great care to protect them against such threat.

That said, you as an employee of Singapore Polytechnic, perform a very important role in maintaining the security and availability of the Polytechnic's ICT Resources. We have written this guide to help explain what you need to do, and what rules you need to comply with, to help ensure that the confidentiality, availability and integrity of the computing resources of the Polytechnic are protected.

This document contains a set of Acceptable Use Policy specifically for staff members. This policy is to ensure that the Polytechnic's computers and networks keep running smoothly and securely.

All Staff of SP are required to strictly comply with the Information & Communications Technology (ICT) Security Policy and Standard issued by the Polytechnic.

2. ICT Security Awareness Training

As a staff member of Singapore Polytechnic, you must receive ICT Security Awareness Training within 6 months of the start of employment. ICT Security Management will coordinate and prepare these training sessions for you but you are responsible to attend these sessions. You must formally acknowledge that you have attended the new-hire training session.

Additionally, you must attend ICT Security Awareness training at least once every year, and you must formally acknowledge that you have attended the appropriate training session.

3. User Accounts

If you need access to ICT Systems to do your job, you will have been issued a SPICE account with a unique User-ID and password. It is very important to understand that this account is for your exclusive use only. You must not share your account with anybody else for any reason whatsoever.

- You must always keep your password secret, and never disclose your password to another person for any reason whatsoever
- You are accountable for all use of the account. This includes, but is not limited to:
  - The contents of all email messages emanating from the account;
  - All instant messaging coming from the account;
  - All social networking postings (e.g. Facebook, Twitter) made from the account;
  - All other forms of information uploaded or downloaded from the account.
- You should be mindful of what you transmit to others from the account, and take great care not to disclose sensitive information of the Polytechnic.
- You must not use or attempt to use someone else's account. You also must not try and monitor another person's data unless you are authorized by your Director to do so.
- You must not access, read, copy, amend or delete another person's files or data without authorization from that person or from your Director to do so.
- Your user account may give you access to certain sensitive information or certain system administrative privileges. If your role within the Polytechnic changes such that you no longer need access to confidential information or need system administrative privileges, you need to inform management so that this access is revoked.
- Your SPICE account will be disabled if unused for 90 days.

4. Passwords

Passwords are the primary mechanism used to guard access to accounts and information. Choosing a good password is very important since the password protects your account and since you are responsible for all utilization of your account.
To comply with Singapore Polytechnic's ICT security policy:

- Never reveal your password to anybody else, for any reason whatsoever[1];
- Never ask somebody else for their password;
- Change your password immediately if you think it's been compromised or if you have given it to another person, no matter what the reason[2];
- Don't write your passwords on a piece of paper or store them in an unprotected file on your computer;
- Comply with the respective password guidelines for your department, for example relating to complexity and change frequency;
- Do not leave your account logged in and unattended; use a screensaver to lock your account when you need to leave your work area for a while.

To comply with Singapore Polytechnic's ICT security policy:

- It needs to be at least 9 characters long;
- It should contain at least 1 letter from the alphabet and 1 number;
- It should not have blanks;
- It should not be the same as your username or User ID;
- It should not be your name or part of your name;
- It should not contain your NRIC/Passport Number;
- It should not contain or be anything that can be associated with you, e.g. your dog's name or street name;
- It should not be a dictionary word.

So, you need to use great care when you pick a password. One easy way to pick one you can remember is to think of a phrase. For example, the phrase "I like Ice Cream" could be converted into a password like 1l1ke1cecream by just putting 1 instead of 'I'; this is a very good password. (Don't use this one though!).

5. Appropriate Use of ICT Assets

The ICT systems, including networks, which have been allocated for your use, are tools to facilitate the business of the Polytechnic. These systems should be usable by you just the way they are, and you must not change their configuration or add/modify/delete any software. Use common sense in what you do on these systems - if it feels wrong, it probably is. When you use the Polytechnic's ICT Systems, you should only use these systems for their intended purpose.

[1] One really good example is a phishing attack, where you get an email asking you to reveal your password. A legitimate site or organization will never ever ask you to reveal your password.
[2] Cases where passwords may be disclosed would include inadvertent disclosure or intentional disclosure to a member of ICT Technical Services in order to resolve a technical issue. In practice, this should never occur.

- Internet access is provided as a tool to help you do your job, and is intended to serve the official purposes of the Polytechnic. The Polytechnic reserves the right to monitor, control and disclose your Internet activities.
- You must not engage in any use or activities that may be considered misuse or abuse
- You must also not break any of the laws of the Republic of Singapore relating to computer use and the use of copyrighted material. In particular, care should be taken to adhere to the following laws:
    - The Copyright Act,
    - The Computer Misuse and Cybersecurity Act;
    - The Spam Control Act.
- If you have any doubt as to the legality of a particular activity, please consult your manager.
- Similarly, you must not upload or download, send or post, enter or publish from or to a Polytechnic ICT Asset (e.g. your notebook) onto local or international Blogs, social networking sites[3], websites, or any other publicly accessible communication channel, anything that is:
    - Distasteful;
    - Objectionable;
    - Fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory;
    - Incite religious or racial intolerance or are otherwise deemed inappropriate;
    - Prejudicial to the good name of Singapore Polytechnic;
    - Illegal as defined under the laws of the Republic of Singapore;
- The Polytechnic's ICT resources are protected with security software and systems, such as antivirus, anti-spyware, personal firewalls, and intrusion prevention systems. You must not interfere with or disable any security related software installed to protect an ICT System.
- Software, when obtained from questionable sources, can be a vector for attack against the Polytechnic. You must not install any unauthorized software onto ICT Systems, and only use software that is licensed for use, legally acquired, and approved by the Polytechnic for use.[4]
- You must comply with the software's licensing agreements when installing and testing software under evaluation
- You must not use the Polytechnic's ICT resources for any commercial purpose or financial gain, unless duly authorized by the Polytechnic in writing.

[3] Social networking sites include sites such as Facebook, Twitter and so on.

[4] For the purposes of this policy, "Licensed for use" includes the right of use associated with freeware, shareware and open source software.

- You must take great care to protect the intellectual property rights of others. If somebody else copyrights something, then you can't copy it without permission.
- To comply with Singapore Polytechnic's ICT Security Policy:
    - You cannot use "peer-to-peer" or "client-to-client" technologies[5], email, FTP, Instant Messaging or any other technology to exchange copyrighted, proprietary information or otherwise infringe on the intellectual property rights of others.
    - You cannot engage in any activities that might expose the Polytechnic to legal action resulting from the apparent misallocation of intellectual property. An example would be to use a photograph on a Polytechnic website without a license to do so.
- You must not engage in any activities that would adversely impact other users or the Polytechnic's ICT Systems at large. These activities include:
    - Trying to deny or degrade another person's access to the Polytechnic's computing resources;
    - Performing any unauthorized hardware or software modifications to any ICT resource for any reason;
    - Installing or using any program, script or device that could cause damage or disruption to the Polytechnic's ICT resources, or which would place excessive load on those resources.

Singapore Polytechnic's ICT network is a very important resource in that it facilitates communication between all of the ICT Systems within the Polytechnic. Hence, great care must be taken as to what is attached to this network.

- You must not connect any non-SP furnished device directly to the staff network. When you use your Non-SP furnished devices[6] you can only connect them to student network or Internet. Non-SP furnished devices can however access staff network only via remote desktop services and using SP authorized credentials.
- If you use Non-SP furnished devices, you are required to secure your Non-SP furnished devices. This includes using of proper authentication and keeping your software up to date to remove any known vulnerabilities.
- You must not run any diagnostic or vulnerability scanning tools while connected to the Polytechnic's networks. In case of a legitimate business need, approval must be sought from ICT Security Manager (ISM).
- You must ensure that third parties, who may be your guests or external contractors, do not connect their devices to the ICT Network without justification and prior authorization[7].

[5] Examples include eDonkey, Gnutella and Bit Torrent

[6] Non-SP furnished devices include desktops, laptop(s)/notebook(s), tablets (also known as slates), smart phones, and storage media such as thumb drives and optical devices (e.g. CD-ROM, DVD).

[7] Authorization to allow SP-appointed contractors/auditors to connect a computer to the Polytechnic's network may be obtained by filling out the ***Visitor SPICE Access Declaration Form***, available on the Intranet.

- You must ensure that neither your SP furnished device nor Non-SP furnished devices are connected to a second network[8] and SP's network at the same time; for example, if you have a USB dongle that facilitates connections to a 3G network, then you can't use that dongle at the same time as your device is attached to the Polytechnic's network.
- You must not set up a wireless access point connecting to the Polytechnic's ICT network without prior authorization from the INDT Network Manager.
- Only authorized portable storage devices furnished by SP, are allowed for use in Whole-of-Government (WOG) PCs. Such devices must not be taken out of SP campus without authorization from CISO.
- The use of portable storage devices on staff PCs shall be minimized by using:
    - On-campus Sharepoint or OneDrive for file sharing between staff
    - eSP (Blackboard) or iChat for file sharing between students

6. Email

Singapore Polytechnic may provide an email account for your use in conducting the business of the Polytechnic. Just like your ICT System account, the email account is for your exclusive use only.[9] You cannot share your email account with any other person for any reason. This means that you are responsible for everything that is emitted from your email account.

You should use the appropriate email systems based on the classification of your email content.

Classification	Secure Email	Staff Email	iChat Email
Secret	✓	✗	✗
Confidential	✓	✓	✗
Restricted	✓	✓	✗
Unclassified	✗	✓	✓

Table 1 - Appropriate email system for each classification of email content

The bottom line when using the Polytechnic's email is to be very careful as to what you write – email is considered to be the same as written correspondence, and is treated legally in exactly the same way. Remember – **email never goes away!**

To be compliant with Singapore Polytechnic's ICT Security Policy:

- The Polytechnic's email services are provided to facilitate the ongoing business of the Polytechnic. Do not use official email for unofficial or personal purposes.
- You must understand that email messages sent and received using the Polytechnic's email system may be accessed at any time by the Polytechnic, when approved by senior management. Examples of when this may occur include

[8] A good example of connecting to a second network is at the same time would be to connect to the SPICE network using a LAN port while at the same time being connected to Wireless@SG on the Wi-Fi port.

[9] It is understood that certain executive level personnel may require that their Administrative Assistants have read access to their email accounts.

investigations of misuse of email accounts or investigations into security breaches of the Polytechnic's ICT assets.

- You should consider email correspondence to be the same as formal written memoranda. This means that all email messages are considered part of the formal records of the Polytechnic and can be monitored by the Polytechnic. **Email messages may even be used in a court of law**. When you write an email, you must keep this in mind, and avoid inappropriate content of all kinds, including the use of inappropriate language.[10]
- You must attach an ownership and legal disclaimer to all email messages, approved by management in your department, whenever the email is transmitted to an external party. SP's approved disclaimer is:

  "This message may contain privileged/confidential information. If you are not the intended recipient, please destroy it and notify the sender immediately. Singapore Polytechnic is not liable for any unauthorized dissemination, copying or use of this message."
- You must not use the Polytechnic's email for:
  - The transmission of Spam or advertising;
  - The solicitation for political candidates;
  - Engaging in illegal or unethical activities;
  - Dissemination of internal email addresses to external mailing lists;
  - The conduct of any personal business.
- When transmitting confidential information, you must ensure that at least the confidential part of the message is encrypted. For example, if you are transmitting a confidential memo in Microsoft Word format, you may encrypt just the document. Consult your Department IT Chairman or the SPICE Service Desk for assistance.
- In the situation where integrity of email content is to be enforced, the email should be digitally signed using SP approved software. Alternatively, the content could be captured in a non-editable format, such as PDF, and enclosed as an attachment in the email.

7. Physical Security of ICT Assets

You are responsible for all SP issued ICT Assets that are in your possession, including notebook PCs, and mobile storage (e.g. Portable Hard Disk, Thumb drive, etc.).These ICT assets form tempting targets for thieves. To be compliant with Singapore Polytechnic's ICT security Policy:

- These ICT assets must never be left unattended.
- ICT assets must be physically guarded against theft. This can be done in a number of ways, including locking the work area when nobody is around, or physically locking devices to something immovable, or physically locking in a secure filing cabinet.
- Take precautions to ensure the safe custody of these ICT assets and of the security-classified information on it.

[10] For additional guidance, please see the section on Appropriate Use of ICT Assets.

- All classified information on these ICT assets should be encrypted to protect the information in case the asset is stolen.
- Except for SP-furnished laptops/notebooks used for official/business purposes, you should not bring any ICT assets out of Singapore Polytechnic's premises. In addition, you should not bring SP-furnished laptops/notebooks for repairs by non-SP authorized contractors.
- Authentication tokens shall not be kept together with the Personal Computers when you bring them out of Singapore Polytechnic's premises.
- You should turn off communication ports, such as Wi-Fi and Bluetooth, when not required.
- When you travel on overseas assignments with these ICT assets, you shall:
  - Ensure only clean ICT assets with minimal information are brought overseas.
  - Check and ensure that these ICT assets can be hand-carried where possible and always kept within sight.
  - If the ICT assets need to be checked-in, ensure all working and classified information in the assets are permanently erased prior to check-in.
  - Be alert at immigration checkpoints and to hold onto your ICT assets until the person in front has gone through the metal detector and should continue to keep an eye on the ICT assets when they go through the X-ray belt and emerge on the other side of the Screener.
  - If security personnel want to conduct checks or see the operation of these ICT assets, you shall insist that it be conducted in your presence. You should never reveal passwords or open up any security-classified information for inspection. On no account, should the assets be taken away. Should you face difficulties with security personnel, you should politely explain that access to these ICT assets need to be explicitly authorized by SP. If necessary, insist on your right to seek assistance from the relevant Singapore Mission or the Ministry of Foreign Affairs (MFA). You can find contact information including 24-hour duty office numbers on the MFA website.
  - If you suspect your ICT assets have been tampered with, you should report it to your IT Chairman and not to connect these assets to SP network.
  - You shall refer to PMO (SNDGO) Circular Minute No. 5/2018 for additional cross border travel guidance.
- If any of these ICT assets is missing or stolen, you must report it immediately to management and an ICT Security Incident report should be completed and submitted by IT Chairman.
- You must ensure that SP data are stored on SP back-end systems with proper backup done. This will ensure that you can continue to work in the event of a loss or malfunction of Personal Computers.
- You shall limit the use to only SP-furnished devices to store classified information. No Non-SP furnished devices are allowed to be used to keep classified information.
- Assigned staff (e.g. Inventory in-charge) shall keep a registry of these ICT assets in department/school and conduct regular checks to account for these ICT assets.

8. Safeguarding Information

Some of the information that you may be exposed to is confidential to the Polytechnic. You need to ensure that this information is protected against unauthorized disclosure at all times. Protection of sensitive information is a very serious matter. Barely a day goes by without a news report relating to mishandling and compromise of sensitive information through carelessness such as misplacing a flash drive with hundreds or thousands of personnel records on it. Such breaches can be avoided with good security practices.

SP also holds personally identifiable information (personal information) within its ICT infrastructure which is confidential, e.g., any information that is unique to any individual or information that is sensitive or proprietary to SP employees and students. Staff with access to personal information must be aware of the importance of maintaining the confidentiality of the information and act to safeguard and not misuse the information.

Information at Singapore Polytechnic falls into four categories. These categories are:

1. Unclassified Information
2. Restricted Information

Unclassified Information is information of a nature which DOES NOT REQUIRE RESTRICTIONS ON ACCESS BY STAFF, STUDENTS OR THE MEMBERS OF THE PUBLIC. Unclassified information is any information prepared, owned, used or retained by the SP for public release and which is not specifically exempt from the disclosure requirements of the applicable laws of Singapore.

Generally, only documents specifically created by SP for the public (e.g., press releases, brochures) and students (e.g. teaching & learning materials), and documents contributed by students related to their course of study are considered Unclassified information.

Restricted Information is information is to be used by SP staff only. Unauthorized disclosure could cause DIFFICULTIES OR UNDESIRABLE CONSEQUENCES TO SP. Any information classified as Restricted must be authorized for external release by the Business/System/Data Owner. Unauthorized disclosure could result in:

(i) Adverse intervention causing difficulties to the normal functions of SP;

(ii) The exploitation of the personal information of any individual in the possession of SP; or

(iii) Embarrassment to SP.

Any information generated within SP shall be categorized as "Restricted" information by default until the proper information security classification can be determined and verified.

If SP's restricted information is to be provided to any third party, the third party must have signed a Confidentiality and Non-disclosure agreement provided by SP and approved by the Business/System/Data Owner.

INFORMATION ASSETS (Default: Restricted)		
Restricted		**Unclassified**
• Agenda and minutes of Board meetings and Standing Committees, (e.g. BOS, BOA, EB, ADC, SPM, ADDS) • External Assessment/Audit reports • Course proposals (prior MOE's approval) • Examination questions (pre-examinations) • Examination solutions (pre-examinations) • Examination Board reports • Examination scripts • Examination results (pre-publication) • Tender documents (pre-publication) and evaluation reports • Sensitive staff / student information (e.g. disciplinary reports, medical reports)	• Agenda and minutes of staff meetings • Agenda and minutes of Joint Poly committees (e.g. JPAC) • Budgetary/ financial information • Circulars • Policies, procedures, standards and guidelines • Corporate work plans • Course documents • Examination marking schemes • Examination papers & solutions(post-examinations) • Information published on the staff portal	• Annual report (published) • Course prospectus (published) • Information published on the SP Website, Student portal • Teaching & Learning materials provided to students • Documents contributed by students in their course of study • Examination papers (declassified post-examinations)

Note: Security classification of personal information shall be determined according to risk, by System/Data Owner

To protect confidential information and ensure your compliance with the ICT security policy:

- You must not disclose Restricted information without first obtaining documented approval from management. An example of documented approval is Confidentiality and Non-Disclosure agreement duly signed by authorized management.

- You should lock all hard copies of Restricted or above information in your desk cabinets when leaving your workstation, and remove it from printers as soon as printed. Such hard copies must always be kept under control.

- You should take appropriate precautions when transporting or transmitting Restricted information to prevent its inadvertent disclosure. Examples include password protecting your MS Office documents, ensuring that classified information is encrypted whilst in transit, and encrypting removable media such as USB Flash Drives so that the data contained within is irretrievable by an unauthorized third party.

- You should make certain that any mobile computing platforms such as notebooks under your control that may contain confidential information are adequately secured. For example, encrypting the sensitive files on such machines or using hard disk encryption is two ways that you can make sure data is safe.

- You must not store classified government data on Non-SP furnished devices.

9. ICT Security Policy Violations

You have a responsibility to report suspected violations to the ICT Security Policy to your IT Chairman. You also need to understand that ICT Security is a serious matter and that there are penalties for policy violations.

To remain compliant:

- When you think there is a violation to ICT Security, or when you think that an ICT Security device or software is not working properly, then you must report it to management immediately.[11]

- When a security incident or system misuse is detected, the Polytechnic's management may decide to conduct an investigation. You need to cooperate with management in every way possible during any investigation. You also need to understand that your user files and Non-SP furnished devices may be examined during the investigation should management deem that this is necessary.

- If violations, such as presence of malware, are detected any SP furnished devices or Non-SP furnished devices, the Polytechnic will deny your connections to the Polytechnic's networks.

- You need to understand that there are penalties for ICT Security Policy violations and/or misuse of ICT Systems. These penalties may include fines, confiscation of devices, withdrawal of access to computing resources, termination of employment and civil action.

- You need to understand that Singapore Polytechnic reserves the right to take disciplinary or legal action against you in the event that you conduct yourself in any manner which is considered by the Polytechnic to be irresponsible; or in the event that you are misusing the computing resources allocated to you.

10. Right of Singapore Polytechnic to Access Data

Singapore Polytechnic maintains the right to access and disclose all data, of any kind, inclusive of email, on all machines owned by the Polytechnic at any time and for any reason. Although the Polytechnic maintains this right, it is only exercised under special situations such as investigating a security breach or ICT system abuse. When such access is required, it is done so with the approval of PCEO.

11. Privacy

Personal data is defined as data that relates to an individual whether in respect of his personal or family life, business or profession, who can be identified from the data or from the data and other information which is in possession of, or is likely to come into the possession of Singapore Polytechnic. Such data is often confidential and may be sensitive. Therefore, the protection of personal data is of utmost importance and active steps must be taken by all information users and custodians to ensure data privacy.

[11] Responsible person may include the Department IT Chairman or the ICT Security Manager (ISM) for the Polytechnic.

All SP staff with access to such personal information must be aware of the importance of maintaining the confidentiality of the information and must act to safeguard and not misuse the information. In particular, SP staff must comply with the following minimum requirements for protection of the personal data that they collect, use, and share or disclose:

a. Obtain consent at or before the collection, use, disclosure or sharing of personal data

b. Specify the purpose for the personal data collection at or before collection. Your purpose statement should explain why you are collecting the personal data, how it would be and could be used and to whom you would be sharing or disclosing the information to

c. Use or disclose the personal only for the stated purpose it was collected and for which consent has been obtained

d. Grant access to the personal data on a need-to-know basis for official work purposes to recipients who have been security-cleared by Dept of Human Resource department

e. Classify and protect the personal data as confidential. Before sharing data with other schools/departments within SP or with Government agencies, make sure that the Data Request Form is completed. Similarly before sharing data with the private sector, make sure that the Confidentiality and Non-disclosure Agreements (NDA) are completed. Do not allow the transfer of personal data overseas unless you can ensure that the same level of protection required by the IM8 Policy on Data Management could be provided by the overseas party to whom the personal data is transferred

f. Specifically, when sending personal data via email, do the following:

    i. Protect the personal data by making use of the Email Information Rights Management System if the personal data is sent within SP. If the personal data is to sent via email outside SP, store the personal data in a Microsoft(MS) Office Word or Excel document and protect it using the MS Office Password Protect feature. Choose a strong password when you protect the document and make sure that the password protected document and password are sent to the recipients in separate emails.

    ii. Check to ensure that the email is address to the correct recipient before sending and make use of mailing list if you regularly sent the email to a specific group.

    iii. Make use of the bcc field when mass mailing to general public.

g. Retain the personal data for the amount of time required by law or regulations or as long as it remains relevant for its primary purpose

h. Destroy the personal data when it is no longer required

i. Do not collect more than it is necessary for your business operations

j. Keep the personal data collected accurate and up-to-date as necessary for the purpose for which they are used

k. Keep up-to-date documentation of how the personal data is used and the parties to whom the personal data is shared with or disclosed to so that you would be able to provide the information when asked by the individual

l. Allow individual to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice, after informing the individual of the implications of such withdrawal

m. Make available information about SP's policies and processes with respect to the processing of personal data in a clear and generally understandable form

12. Compliance Audit

Your Compliance to this Acceptable Use Policy may be audited by the ICT Security Team. Non-compliance will reported to CISO for further action. The frequency of this audit is annual and staff will be randomly selected to verify compliance.

User Acknowledgement

I hereby acknowledge that I have read this SP ICT Acceptable Use Policy and that I understand its contents. I further acknowledge that I will strictly comply with the policy detailed in this document.

Name: ______________________________

Title: ______________________________

Department: ______________________________

Date: ______________________________

Signature: ______________________________