Samoa Land Corporation

Information & Communication Technology (ICT)

Policies, Regulations and Guidelines

Introduction

ICT the vast and growing array of computing and electronic data communications facilities and services is used daily to create access, examine, store, and distribute material in multiple media and formats. ICT plays a vital part in the fulfilment of SLC research, administrative, and other roles. Users of SLC ICT resources have a responsibility not to abuse those resources as well as maintain the integrity and security of these resources (equipment and data).

Purpose:

To provide guidelines for the Corporations' hardware and software, computer network access and usage, internet and email usage, and security and privacy for users of SLC.

Objectives:

- Ensure the security of personal, privileged, or otherwise sensitive data and resources that may be processed in any manner by the Samoa Land Corporation.
- Provide uninterrupted network resources to SLC users.
- Ensure proper usage of networked information, programs and facilities offered by SLC networks.
- Secure email from unauthorized access.
- Protect the confidentiality and integrity of data and programs from unauthorized users and access.
- Protect the confidentiality and integrity of data and programs from potentially harmful infiltration by mal-ware (viruses, Trojan horses, worms etc).
- Provide Internet and email access to the users of SLC networks.
- Minimise costs due to unsolicited e-mails (chain-letters, spam etc).

Scope:
This Policy applies to all employees who have been provided access rights to the SLC ICT resources and compasses the use of Printers, Copier, Personal Computers, computer network resources, internet access; Office e-mails accounts and electronic backups.

Information Technology Policies and Regulations

A. Network Resources (Hardware and Software and SLC Server)

Prohibitions

i. Sharing any information that is confidential by law, rule or regulation.
ii. Unauthorized installation of software
iii. Unauthorized Installing and/or sharing of printers
iv. Unauthorized replacement of hardware or software.
v. Unauthorized attachment of processing devices. (eg CPU, ROM, Memory Card)
vi. Using network resources to play or download games, music or videos that are not in support of Corporation's functions.
vii. Downloading *software*, pictures, videos and music.
viii. Movement of any hardware unauthorized.
ix. Storing files that are not work related on the SLC Server (music/games/movies).
x. Attaching privately owned personal computers or other IT resources to the network.
xi. Modifying hardware or software.
xii. Unauthorized uploading of files.

Other jobs to look at:

a) Scanning any removable media for viruses before use (USB flash drives, etc).
b) Running viruses scan every beginning or end of week.
c) Update Antivirus every month.
d) Notify Principal IT Officer when there is an error with the internet, email, network, software or hardware (Includes printers, scanners, UPS).
e) Switch off all PC and UPS after work.
f) Turn off SLC Servers, Telephone System and disconnect Internet end of day Friday every week and turn on again Monday the following week.
g) Notify Principal IT Officer when there is a need of the internet, Land Management System or Servers on weekends.
h) Systems check to optimize performance and scanning of disk drives for errors.

B. Samoa Land Email Account

Email accounts access are provided to users to assist them in performing the duties and responsibilities associated with their positions. Emails sent from SLC email accounts are official correspondence and should be written and treated as such.

Guidelines for use of emails

i. Emails must utilize correct corporate style for a normal correspondence.
ii. Email signatures should include writer's name, designation, division, Corporation name, telephone & fax numbers, address, website and e-mail disclosure.
iii. Proper email protocol rules should be followed.
iv. All emails received should be answered straight away.
v. Response priority should be.
vi. Emails should only be cc'ed when needed.
vii. Emails should only be bcc'ed when needed
viii. Automatic reply email must be generating for staff on Leave/Sick etc.

Prohibitions

a) Sending unsolicited / unwanted junk email, chain letters of all kinds (jokes, prayers, Power-point photo presentations, advertising.
b) Receiving and subscribing to non-work related
c) Sending any material that contains viruses, Trojan Horses, worms, time bombs, cancel bots, or any other harmful or deleterious programs.
d) Any emails that incite violence and hatred against any individual or group of people.
e) Any emails that discriminate against employees by virtue of any race, gender, nationality, religion, and so forth, will be dealt with according to the harassment policy.
f) Any emails containing pornographic material (photographs, videos, jokes or stories).

SLC Staff

i. A new email account will be created for a new SLC staff member.
ii. Email account will deactivate straight after termination of service.
iii. Employee will be responsible for his own back up files when terminated.
iv. Users are responsible for maintaining the security of their own PC and email accounts and passwords.

C. *Internet Access*

Internet access is provided to network users to assist them in performing the duties and responsibilities associated with their positions.

Prohibitions

a) Using any forms of Online Social Media Network website with unrelated work.
b) Using the Internet for broadcast audio for non-ministerial use.
c) Using the Internet when it violates any law.
d) Pornography
e) Intellectual Property Right infringement (downloading, copying and/sharing music, video, photographs or other media including software that is protected by intellectual property legislation).
f) Downloading files from unknown or suspicious sources (movies, mtvs, software)
g) Online Gambling and gaming.
h) Watching online videos.
i) To incite violence and hatred or discrimination.

D. Access to Network Files

The File Server is where all staff members should save their work related documents. Media files such as Movies, Photos and Music is prohibited on the server, if any of these kinds of files are found on the server it will be deleted immediately without any notice by the Network Administrator. All staff members have their own Personal Folder on the server and this folder is only access by each staff member. Reminder staff members are not allowed to save any media files in this folder. Each division will have their own folder to save their data; the purpose for this is for data sharing within the division.

Prohibitions

a) Saving non work related media files such as photos, music, videos on the server.
b) Allowing unauthorized people to access the server.
c) Attempting to access folders or files to which a user does not have authorization.

E. Security of Electronic Systems

Samoa Land Corporation maintains electronic communications, electronic media and other computer systems to assist in the conduct of business within the Corporation. All software and hardware are Samoa Land Corporation's property and all messages or files composed, sent, or received on it are, and remain, the property of the Samoa Land Corporation.

Prohibitions

Associates are strictly prohibited from sending electronic communication or otherwise using the Company's electronic media services or computer systems in connection with any of the following activities:

a) Engaging in illegal, fraudulent, or malicious activities;
b) Sending or storing offensive, obscene, or defamatory material;
c) Annoying or harassing other individuals;
d) Using another individual's account or identity without explicit management authorization;
e) Attempting to test, circumvent, or defeat security or auditing systems, without prior authorization;
f) Permitting any unauthorized individual to access the Company electronic System & Company's computer.
g) Discussing proprietary or confidential information;

h) Discussing pending or anticipated litigation or regulatory action with any party other than Company

The Principal IT Officer provides access right to all Electronic System users, the level of access right will decided upon request from Manager Corporate Services or the Assistant Manager Account.

F. Backup and Storage of Electronic Data Files

It is every employee's responsibility to ensure that all data and files that have a continuing value to the Samoa Land Corporation are stored on designated Folders assign for each section on Server, so they can be backed up on a regular basis by the Principal IT Officer.

Backups procedures for the following Systems:

Land Management System.

1. Generate backup after daily posting (EOD Backup) once.
2. Generate backup before end of last working day of each week (EOW Backup) once.
3. Generate backup after monthly posting and adjustment on the last working day of each month (EOM Backup) once.

Attache' General Ledger

1. Generate backup before end of day (EOD Backup) once.
2. Generate backup before end of week (EOW Backup) once.
3. Generate backup before end of month (EOM Backup) once.

Infinity Point of Sale System

1. Weekly checks and follow ups carried out for smooth running and proper performance on Monday every week.
2. Issues and Fault should be reported straight away and digicel support group will be informed for recovery.
3. Irregularity report submitted within 24 hours of the incident.
4. Generate backups weekly on every Friday.
5. Generate backups monthly every last day of the month.

Backups are copied to company external hard drive and sent to off-site storage on a monthly, quarterly, and annual basis.

Backup may be removed (deleted) after five years and must be confirmed first from each Department Managers the removal of such files. Removal of this material will reduce the amount that is required to be included in each of these backups.

Common Forms of Computer Abuse

- Privacy
- Reading another user's files (protected or not)
- Deliberate, unauthorized attempts to access or use SLC's computers, systems, or data
- Theft
- Using deception to avoid computer use charges
- Deliberate, unauthorized use of another user's account or files
- Abusing specific resources
- Removing any equipment (hardware, software, data) without authorization

- Copying or attempting to copy data or software (protected or unprotected) without proper authorization
- Interfering with legitimate work of another user (via computer or in person)
- Sending abusive or obscene messages via computers
- Miscellaneous
- Unauthorized and time consuming recreational game playing
- Using computer accounts for work not authorized for that account
- Sending chain letters or unauthorized mass mailings
- Personal advertisement
- Removal or deletion of software without authorized permission
- Installing abusive or obscene software or files
- Unauthorized attempts to replace computer or printer components
- Unauthorized attempts to repair or tamper with computers or printers

COMPUTER USAGE GUIDELINE

- Users are to have valid, authorized accounts and may only use their account in accordance with its authorized purpose. Users should not let another person use their account.
- A user may not change copy, delete, read, or otherwise access files or software without the explicit permission of the Administrator.
- A user may neither prevent others from accessing the system nor unreasonably slow down the system by deliberately running wasteful jobs or programs, sending mass mailings, or chain letters.
- Users should assume that software they did not create is copyrighted. They may neither distribute copyrighted or proprietary material without the written consent of the copyright holder nor violate copyright or patent laws concerning computer systems (hardware/software).
- Users must always change their password for each month for security purposes, and avoid other user's login into their account without their knowledge.
- Users must not deliberately introduce any virus or worm or any other nuisance program or file on to the system that can harm or infect the servers/system.

Enforcement

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