SAMOA FIRE & EMERGENCY SERVICES AUTHORITY

INFORMATION TECHNOLOGY (IT) POLICY 2020

Table of Contents

LIST OF ACRONYMS

CSD:	Corporate Service Division
HR:	Human Resource
HRD:	Human Resource Division
ICT:	Information Communication Technologies
ID:	Identification
IRF:	Internal Requisition Form
ISC:	Intranet Steering Committee
ITD:	Information Technology Division
ITP:	Information Technology Policy
OIC:	Officer in Charge
PABX:	Private Automatic Branch Exchange
PC:	Personal Computer
PPD:	Policy and Planning Division
SFESA:	Samoa Fire and Emergency Services Authority
SSO:	Senior Station Officers

DEFINITION

Intranet:	Internal shared folders used by the Authority
Message boards:	Pop up messages on the screen which are also a form of virus which will cause some damage to the computers
Viruses:	Programs that can damage or destroy files within the computer
Intranet Steering Committee:	Comprises of the Commissioner, Assistant Commissioners and Manger Corporate Services
User:	Refer to employee[1] who 'uses' the Authority Information Technology Resources and equipment
Executive Management:	Comprises of Commissioner, Assistant Commissioners, and Manager Corporate Services

[1] Defined in HR Manual of Instruction 2019

1) INTRODUCTION

The Authority aims to assist its employees in implementing its duties, roles and functions by providing Information Communication Technologies (ICT's) and resources varying but not limited to phones, emails, internet, computers, and laptops

The provision of these ICTs has its limitations due to budget constraints, therefore this Policy provides guidelines and procedures to allow effective and efficient use of such resources.

This ensures that proper management of the ICT equipment and resources and that they are used appropriately and maintained accordingly to prolong its lifespan for use of the Authority.

2) POLICY STATEMENT

The guidelines within this policy aim to provide effective and efficient support services to the Authority through information technology.

The Policy and Planning Division(PPD) and the Information Technology Division (ITD) reserves the right to modify these guidelines at any time to address issues that have been missed in the current policy and to ensure this policy is in line with the evolving changes of information technologies.

For questions or comments, please contact ITD on email administrator@sfesa.ws or Policy Division on email policy_division@sfesa.ws

3) PURPOSE/AIM

a) The ITP (Information Technology Policy) provides guidelines and procedures for ALL users of SFESA to follow and adhere to.

b) Ensures that information technology equipment and resources are used appropriately and well taken care of to allow maximum use and prolong the lifespan of these equipment.

c) Create security standards to protect the Authority's resources and information from being infected by computer virus and hackers

d) Enables the ITD to manage the IT equipment and resources and how they have been utilized thus leading to Improving the quality of work and employee productivity

4) AUDIENCE

This document applies to ALL employees, whom from here on throughout the document will be referred to as User who use resources and information technology equipment owned, leased or

hired by the Authority regardless of the time of day, location, or method of access. These users are mainly;

- Commissioner
- Assistant Commissioners/ Manager Corporate Services
- Commanders and Principal Officers
- Senior Officers/Senior Station Officers (SSO's)
- Officers/ Officer in Charge (OICs); and

Not limited to the above users, other employees within the Authority may also become users and must adhere to this policy. Any third party such as Visitors, volunteers, Project Contractors, Consultants or Suppliers must have prior authorization from Executive Management of the Authority to use ICT resources including Internet or Mail resources and networks.

5) OWNERSHIP

1. The Authority has all the rights and owns all the resources and equipment mentioned and outlined under this policy

2. It is the Users responsibility to take ownership of appropriate use and care of such resources they use daily to achieve their work under the Authority

3. The ITD is the core division managing the guidelines within this policy to ensure it is being implemented and practiced by SFESA staff with support of the Policy and Planning Division

6) USER RESPONSIBILITIES

1) It is the responsibility of ALL users to maintain and utilize **All** IT equipment of the Authority in accordance with the guideline within this Policy. It is also their responsibility to ensure that no unauthorized user has access to the Authorities IT equipment and resources whether in their care or not.

2) Users are strictly prohibited from discussing and sharing any official or confidential Authority business and information on any social media site that may harm the Authority otherwise they will be dealt with under the SFESA HR Manual of Instructions 2019.

7) EMAIL AND MESSAGING

Objective: Provides appropriate guidelines in utilizing the Authority's email system and Messaging Services.

Applies to: All Users

Email and messaging are important and sensitive business tools. This guideline includes all electronic messages composed, sent or received by any user that is using the Authority's electronic messaging and email services.

7.1 Prohibition on use of email and messaging systems;

a) The list below outlines what is considered to be inappropriate use of email and messaging system and are prohibited for all users. Use of email or electronic messaging systems for transmitting movies, messages containing pornography, profanity, derogatory, defamatory, sexual, racist, harassment or offensive materials.

b) Using of provided electronic messaging resources for any promotion or publication of one's political or religious views or for the operation of a business or for any undertaking for personal gain.

7.2 Accessibility

a) The Authority provides electronic messaging and email resources to assist with its daily businesses
b) ITD will also create and automatic electronic email signature for ALL users indicating the Authority Logo, phone numbers, fax rand links to the website and shall assist each user in personalizing the signature to indicate name of each user, position or occupation.
c) All messages composed and/or sent using the Authority's provided electronic messaging resources must comply with policies regarding acceptable communication[2]
d) If a user resigns or is terminated from the Authority, the employee will be denied all access to electronic messaging resources immediately, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient after he or she leaves the Authority. Any employee who discovers a violation of these criteria's should immediately notify ITD

7.3 Ownership

a) The email/ electronic messaging systems including ALL messages stored, composed, sent or received in the Authority's provided electronic messaging system(s) becomes the property of the Authority. Electronic messages are NOT the property of any employee.
b) The Authority reserves the right to intercept, monitor, review and/or disclose any message composed, sent or received if appropriate and/ or required by the Commission for an investigation
c) The Authority reserves the right to alter, modify, re-route or block the delivery of any messages as it deems inappropriate.
d) The unique email addresses and/or instant messaging identifiers assigned to any employee or user are the property of the Authority. Users must utilize these identifiers appropriately and at all times while employed by the Authority

7.4 Confidentiality

a) Messages sent electronically can be intercepted from people inside or outside the Authority and as such there may be a breach into the system. Employees of the Authority

[2] Referring to the Ministry of Communication and Information Technology Government Internet and Electronic Mail Policy 2016

must not disclose proprietary or confidential information through email or instant messages.

b) Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically vis-à-vis delivery in person.

c) Electronic messages are legally discoverable and permissible as evidence in a Court of Law. Messages should not be composed that you would not want to be read out loud in a court of law in such occasions.

d) All users must not disclose proprietary or confidential information of the Authority through email or instant messages

e) Users are prohibited from unauthorized transmission of the Authority's trade secrets, confidential information, or privileged communications.

f) Unauthorized copying and distribution of copyrighted or confidential materials is prohibited.

7.5 Security

a) The Authority employs sophisticated anti-virus software. Users are prohibited from disabling anti-virus software running on any provided computer or network equipment.
b) Although the Authority employs anti-virus software, some virus infected messages can enter the Authority's messaging systems. Viruses, "worms" and other malicious codes can spread quickly if appropriate precautions below are not followed;

i. Be suspicious of messages sent by people not known by you.
ii. Do not open attachments unless they were anticipated by you. If you are unsure, always verify the sender is someone you know and that he or she has actually sent you the email attachment.
iii. Disable features in electronic messaging programs that automatically preview messages before opening them
iv. Do not forward chain letters, just simply delete them.
v. Do not attempt to remove yourself from future delivery of such a message that you determine is spam. These "Remove Me" links are often used as a way to verify that you exist. The Authority considers unsolicited commercial email spam and a potential security threat.
vi. Do not use the Authority's provided email address when posting to message boards as Internet message boards are a fertile source from which mass junk e-mailers harvest addresses and email domains.

8) INTERNET USAGE

Objective: Provide appropriate guidelines for accessing and utilizing the Internet through the Authority's Network.

Applies to: All users who are authorized access to Internet services

Internet services are authorized to designated users by their managers to enhance their job and responsibilities. The Internet is an excellent tool but also creates security implications that the Authority must guard against. For that reason, users are granted access only as a means of providing support in fulfilling their obligations under the Authority.

8.1 Prohibited use

The following use of the Authority's Internet access are prohibited:

a) To access, upload, download, or distribute movies, pornographic or any material that is sexually explicit in nature
b) Vandalize or damage the property of any other individual or organization
c) To invade or abuse the privacy of others
d) Violate copyright or use intellectual material without permission
e) To use the network for financial or commercial gain
f) To degrade or disrupt network performance
g) Utilization of the Authority's facilities knowingly to download or distribute pirated software or data.
h) The use of file swapping software on computers and the Authority's network
i) Utilization of Authority's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
j) Unauthorized access as per management directives from time to time
k) Discussing and sharing any official or confidential Authority business and information on any social media site that may harm the Authority. Otherwise they will be dealt with under the SFESA HR Manual of Instructions 2019

8.2 Internet access and ownership

a) Internet accounts are approved for designated employees or users by their Supervisors (SFESA Management) as a tool to assist in their line of work.
b) The ITD will take responsibility for all web site content (i.e., "the Authority's web site") and format presentation to reflect the Authority's mission and in supporting its departmental objectives.
c) Any software or files downloaded via the Internet into the Authority's network becomes a property of the Authority Any such files or software may be used only in ways that are consistent with their licenses or copyright laws

8.3 User responsibilities

a) Each user is responsible for the account issued to him/her.
b) Sharing Internet accounts or User-ID's is prohibited.
c) The utilization of Internet services must be to support the user in achieving Authority services and support legitimate mission related to activities of the Authority and be consistent with prudent operational, security, and privacy considerations.

9) PASSWORD SECURITY

Objective: Provide guidelines for appropriate management of the Authority passwords and to maintain adequate security and integrity of all of the Authority's Information systems.

Applies to: All users

9.1 Importance of passwords

a) Maintaining security of the Authority's business applications, software tools, email systems, network facilities, and voice mail are critical in providing data integrity and stability of the systems.
b) Passwords are provided to limit access to these assets on an ''as needed basis''.
c) The Commissioner has the authority to override any password as it sees fit for the purpose of the efficient operations of the Authority.

9.2 Provision of passwords

a) The Authority provides access to network, electronic mail and voice mail resources to its users in support of its mission.
b) Passwords are assigned for access to each of these resources to authenticate a user's identity, to protect the network users, and to provide security.
c) New employee passwords and changes must be requested by the Executive Management. This helps monitor and manage the importance of password distribution and usage in such a way that reinforces the integrity of users accessing the Authority's system
d) ITD must oversee any password change requested by a user's supervisor. Confirmation will be sent to a user when a password change is completed at the request of a supervisor
e) ITD will handle requests from the Authority Executive Management team.
f) Password account requests must be verified by the employees upon notification from Human Resource Division (HRD)

9.3 User and ITD responsibility

a) It is the responsibility of each user to protect and to keep private any and all passwords issued to him/her by the Authority. This will assist the Authority as it strives to manage secure computing networking environment, although it cannot guarantee the confidentiality or security of the network, e-mail or voice mail passwords from unauthorized disclosure, these simple responsibility by the users will be of assistance to the ITD.
b) A user may log on to another users machine if required for work related purposes. This must be approved by the Commissioner.
c) System administrator must protect confidentiality of user's password
d) Users must manage passwords accordingly to the password guideline below
e) User is responsible for all actions and function performed by his/her account
f) Suspected password compromise must be reported to ITD immediately
g) The ITD will delete all passwords of exiting employees upon notification from HRD

h) ITD will automatically send ALL users to Change their password periodically (every 3 months)

9.4 Password Guidelines

This is a brief outline of how to select a password and ensure no one else knows your password

a) Selecting a Wise Password

The employee or user must create a password that follows the criterions below;

i. Do not use any part of the account identifier (username, login ID, etc.)
ii. Use 8 or more character
iii. Use mixed alphabet and numeric characters For Example: Johnathan345

b) Keeping Your Password Safe;

i. Do not tell your password to anyone
ii. Do not let anyone observe you entering your password
iii. Do not display your password in your work area or any other highly visible place
iv. Do not reuse old passwords

c) Additional Security Practices

i. Ensure your workstation is reasonably secure in your absence from your office.
ii. Consider using a password-protected screen saver, logging off or turning off your monitor when you leave the room.

10) INTRANET USAGE

Objective: Provide guidelines for the appropriate use of the Authority's Intranet to improve the productivity and effectiveness of our staff and to maintain security of our Intranet assets

Applies to: All users

The Authority's Intranet is a Server SHARE folder based source of file sharing for our internal employees or users. Security measures must be established to allow users access to appropriate sections of the Authority's Intranet to assist with their efforts in conducting business for the Authority. The Intranet Steering Committee are responsible for setting the goals and objectives for the Authority's Intranet, determining priorities for adding new content, and for maintaining the integrity of the Intranet and maintaining consistent format for all web sites and pages developed for the Intranet regardless of original department source. Each of the Authority's operational and support departments will be represented in The Intranet Steering Committee to provide content and processes that enhance employee knowledge and productivity. Employees are to submit feedback and suggestions to their Department representative.

10.1 Access

a) All authorized users of the Authority are approved access to the Authority Intranet. Part time employees and contract employees must have ISC approval for Intranet access.

b) Intranet security passwords are the responsibility of each individual authorized to access the Intranet. Passwords are not to be shared, swapped, or given out in any form and must be kept hidden from others (if written on paper) but ITD highly recommends employees to memorize their passwords.
c) The Authority will provide security access based on Active Directory Usernames that will be the employee's access code.
d) Only users of a Department has access to their Share folder.

10.2 Authorized material on the Intranet are as follows;

a) Departments may include links in department sites/pages for downloading
b) Documents and files in the following formats:
   i. Microsoft Excel
   ii. Microsoft Word
   iii. Microsoft Access
   iv. Microsoft PowerPoint
   v. Adobe PDF
   vi. Visio
   vii. Images and video files approved by the Management

10.3 Ownership

a) All content residing on the Authority's Intranet is the property of Authority.
b) Downloaded files from the Intranet are considered proprietary information of the Authority and should be treated as such.
c) Our Intranet represents an ongoing reflection of the Authority's structure.

10.4 User and administration responsibilities

a) It is every employee's right and obligation to provide input that constantly improve and update the accuracy of all content materials.
b) Maintenance of the Intranet is the primary role of the ITD.

11) PHONES

Objective: Provide guidelines on appropriate use of the Authority's phone system to maintain high productivity and cost effective results.

Applies to: All users

The two types of phone services used by the Authority are Office phone system and cell phones and both have different issues and require unique guidelines for clarity. Phone systems and equipment's are provided to enhance user's capability in conducting the Authority's businesses effectively and are not to be considered as assets available for personal use. The following guidelines should be fully understood and practiced by all employees.

a) Authority's Phone System are assets to assist in conducting the Authority's business.

b) Local phone provider will be determined by the Manager CSD along with ITD and Communication Division responsible for supporting the PABX (Private Automatic Branch Exchange) telephone systems.
c) The Authority's telephone numbers are to be used for the Authority's business during business hours and all calls should be answered if the employee is in the office at the time
d) Office phone maintenance and replacements will be conducted by the ITD with assistance from the Communications Division when needed. In the case that both divisions cannot fix the problem an external phone company will be contacted for way forward.
e) Be courteous and considerate when representing yourself and the Authority when using phone services.
f) Long distance calls can accumulate to significant costs. The Authority monitors long distance calls of every department as a means of managing phone expenses just as it does with other Authority expenses.
g) Personal phone calls made using the Authority telephones are **not** allowed.
h) Personal long distance calls are **not** allowed and is the responsibility of the employee.
i) Personal calls are **not** allowed on office private lines (NECC and Station Watchrooms). These telephone lines are specifically for contacting emergency callers.

11.1 Cell phone

Cellphones are provided only for the Executive Management and these users must know and adhere to terms and conditions of their employment contracts related to cellphone;

11.2 Losses and repairs

a) The HRD are the Cell Phone Contract Administrator whom must be notified immediately when a cell phone is lost or stolen so that appropriate action can be taken with the cell phone provider.
b) All cost related for repairs and damages to cell phones are the responsibilities of the user.

11.3 Replacements

If the equipment is defective, the cellphone provider will replace it at no cost to the user, however if the equipment is damaged through negligence on the part of the user, then additional costs may be incurred. All replacement requests are processed in coordination with the Cell Phone Contract Administrator.

12) PC SOFTWARE STANDARDS AND UTILIZATION

Objective: Provide guidelines for purchasing and installing software on the Authority's PC's as well as what's considered appropriate utilization of such software.

Applies to: All users

These guidelines is intended to ensure that all employees understand that no Computer software may be loaded onto or used on any computer owned or leased by the Authority unless the software is the property of or has been licensed by the Authority.

12.1 Requesting Standard PC Equipment and Software

a) Equipment and software requests will be provided quickly as long as appropriate approvals are granted. These steps outlines the process for purchasing PC equipment and Software:
   i. Complete the PC Equipment or Software Request Form/ Internal Requisition Form (IRF)[3].
   ii. Supply approval from relevant Output Manager[4]
   iii. Submit request to IT divisions for evaluation.
   iv. The ITD will review the order and forward to the Finance Division or will contact the requesting division for clarification as needed.
   v. The ITD or Finance Division are available for follow-up

12.2 Variance Request

Request for a variance for the provided PC Hardware or Software must follow the below procedure;

a) Complete IRF.
b) Practical and sufficient justification is a key part so be concise in building your case for deviating from the standard.
c) Gain approval of the request from your Department Manager.
d) Submit the request to the ITD for review. Your request is reviewed and either approved or declined based upon justified
e) Reasons presented and the ITD's ability to support the new configuration within the Authority's Network will be highly considered for the request.

12.3 Software purchase, duplication or copyright guidelines

a) Software purchased by the Authority or those already residing on the Authority owned computers is to be used only within the terms of the license agreement for that software title. Unless otherwise specifically provided for in the license agreement, any duplication of copyrighted software, except for archival purposes is a violation of Copyright Laws.
b) To purchase software, users must obtain the approval of their department manager who will follow the same procedures used for acquiring other assets. All approved software will be purchased through the Finance Division.
c) The Manager CSD and the ITD will be the sole governing body for defining appropriate software acceptable for use of the Authority while taking into consideration the request and justifications of the user.
d) Under no circumstances will third party software applications be loaded onto the Authority owned computer systems without the knowledge or approval from the ITD.
e) The Authority does not condone the illegal duplication of software in any form. Illegal reproduction of software is subject to civil and criminal penalties, including fine and imprisonment.

[3] Refer to SFESA Finance Policy and Procedural Manual 2019 to obtain the form
[4] Refer SFESA Finance Policy and Procedural Manual 2019 for Output Managers

f) Users are prohibited from giving Authority acquired software to anyone who does not have a valid software license for that software title. This shall include but is not limited to clients, vendors, colleagues, and fellow employees.
g) Any users who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the HR code of Conduct and may include termination of employment.
h) Any user who determines that there may be a misuse of software within the Authority will notify the ITD (Software manager) or his/her immediate Supervisor.
i) All software used and purchased by the Authority for its computing devices, will be acquired through the appropriate procedures practiced by the finance division[5]

12.4 ITD's Role in the Purchase of Hardware and Software

a) Assist departments with evaluating new business software solution
b) Act as liaison for departments when dealing with computing vendors
c) Recommend and evaluate the tasks/jobs/functions to be accomplished via the new software product
d) Assist with hardware and system requirements
e) Install the software as needed
f) Enforce Authority hardware and software standards

12.5 Software Utilization

a) Users will utilize all software in accordance with its license agreements. Anyone found copying software other than for backup purposes is subject to disciplinary action
b) Legitimate software will be provided to all users who need it. The Authority users will not make unauthorized copies of software under any circumstances.
c) Each user of software purchased and licensed by the Authority must acquire and use that software only in accordance with the applicable Software License Agreement.

12.6 Software Registration and Installation

a) Software purchased by the authority will not be registered in the name of an individual. When the software is delivered it must be properly registered by the ITD
b) Software must be registered In the name of the Authority with the job title or department name in which it is used.
c) After the registration requirements above have been met, the software may be installed into the Authority equipment's. A copy of the license agreement will be filed and maintained by ITD.
d) Once installed, the original installation media should be kept in a safe storage area designated by the ITD
e) Shareware software is copyrighted software that is distributed freely through bulletin boards, online services, and the Internet. Shareware payment will be the responsibility of the Authority
f) Installation and registration of shareware products will be handled in the same way as other software products that may be required by the Authority such as Photoshop

[5] Outlined in the SFESA Finance and Procedural Manual 2019

12.7 Software Audit

a) ITD will conduct audits every 6 months for all Authority owned PCs, and laptops to ensure that the Authority is in compliance with all software licenses.
b) Audits will be conducted using an auditing software product.
c) Software for which there is no supporting registration, license, and/or original installation media will be removed immediately from the user's computer.
d) During these audits, the ITD will search for computer viruses and eliminate any that are found.
e) The full cooperation of all users is required during software audits.

12.8 Software standards

The following software standard have been established to ensure all software are up to standards need by the Authority and also to ensure efficient and cost effective use of Authority's computing assets:

a) To provide more effective system administration
b) To assist in the computer planning process and enable the realization of Long term goals and the future computing vision
c) To ensure cost effective purchasing
d) To enable effective tracking of software licenses
e) To provide cost effective user software training for newly installed computer software
f) To facilitate efficient and effective technical support effort

12.9 Technical Support

a) ITD's role In the purchasing of Hardware and Software is to provide assistance with evaluating new business software solution
b) Software support is provided at several levels and is based on whether the software is the requested and needed by the Authority and its various department specific software
c) The ITD will not provide support for evaluation software, personally purchased software, illegal copies of software screen savers, shareware, and non-network software that is not included in the standard software list.

12.10 Standard PC Equipment and Software

a) Standard PC hardware and software configurations are posted on the Authority's intranet website in the ITD section and will change from time to time given evolving and improved technologies thus there is no set list. If a user requires this information ITD can be contacted for further questions

12.11 Repairs and Maintenance

a) It is the responsibility of the user to maintain the Authority's IT
b) All users must report faulty IT tools and equipment to ITD within 24 hours of fault. Reports must be submitted in the authorized Authority Report Form[6] Report must state problem or fault and cause of problem.
c) All reports must be endorsed by the relevant Output Manager.

[6] Refer HR Manual of Instructions for Report Form Template

d) All IT tools, equipment and software repairs must be approved by the Manager: Corporate Services prior to repairs.
e) ITD staff are responsible for repairs and maintenance of all Authority IT Tools Equipment and Software.

13) BIOMETRICS

Objective: Provide guidelines for appropriate management and utilization of the biometrics machine to monitor users working hours

Apply to: All users

Biometrics is an initiative established in the Authority to avoid working time disputes and fabrication given many issues in the past also picked up the Auditors. These guidelines are intended to ensure that all users understand why they need to utilize the biometrics. The biometrics is a fingerprint device used by all employees of the Authority to clock in and clock out.

a) The biometric devices are assets to assist in conducting the Authority's sign in and sign out of staff.
b) Once someone scan his or her fingerprint biometrics are able to record information such as employee number, first name, last name, assigned station and time at which the fingerprint was lodged.

13.1 ITD Responsibilities

a) ITD is responsible for registration of every member of the Authority in order to have valid fingerprint scan that links to the biometric device.
b) Biometric device maintenance and replacements will be conducted by the ITD with assistance from Comptec Company Ltd if needed. In because Comptec is the only company that imports the recommended brand of the device which is REALAND.
c) Biometrics are to handle with care, requires clean hands in order for the device to successfully operate.
d) Biometric data is confidential that only the ITD and MCSD can have access to it.
e) Permission for issuing of biometric data by individual will have to request approval by the Commissioner. Basic instructions on how to use biometrics machine and when is attached as **Annexre 1**.

ANNEXURE 1

SIGN IN/OUT PROCEDURES WITH BIOMETRICS MACHINE

1. FOR NORMAL WORKING HOURS:

To Sign In:

1. Press F1 Button
2. Put Finger/Thumb on Scanner
3. Release Finger/Thumb from Scanner

To Sign Out:

1. Press F2 Button
2. Put Finger/Thumb on Scanner
3. Release Finger/Thumb Scanner

2. FOR COVER SHIFT/ON CALL WORKING HOURS:

To Sign In:

1. Press F3 Button
2. Put Finger/Thumb on Scanner
3. Release Finger/Thumb from Scanner

To Sign Out:

1. Press F4 Button
2. Put Finger/Thumb on Scanner
3. Release Finger/Thumb Scanner

NOTE:

1. For Daily Workers who is approved overtime work, there is no need to use option for Cover shift, please use normal sign in/out procedure as stated in #1.

2. Duty Crew Officers in Charge to advise Corporate Services on staff members who are on Annual and Sick Leave

3. The Authority will not be liable for staff members hours if fail to sign in or sign out.

Developed and published by the Policy and Planning Division & Information Technology Division of the Samoa Fire & Emergency Services Authority (SFESA).