PERSONAL INFORMATION AND DATA PROTECTION GUIDANCE

JUNE 2016

Table of Contents

INTRODUCTION

Under the National Information Technology Development Agency (NITDA) Act of 2007, Government departments, Offices, Agencies and non-governmental organizations as data controllers, have a legal responsibility to:

- obtain and process personal data fairly;
- keep it only for one or more specified and explicit lawful purposes;
- process it only in ways compatible with the purposes for which it was given initially;
- keep personal data safe and secure;
- keep data accurate, complete and up-to-date;
- ensure that it is adequate, relevant and not excessive;
- retain it no longer than is necessary for the specified purpose or purposes; and,
- Provide a copy of his/her personal data to any individual, on request.

The purpose of these guidelines is to assist FAROF in implementing systems and procedures that will ensure, as much as possible, that personal data in their possession is kept safe and secure and to help FAROF, Offices, Agencies and non-governmental organizations meet their legal responsibilities as set out above. This document is a guide and can be expanded upon by FAROF to create detailed policies and procedures which reflect specific business requirements.

Any queries in relation to the content of this document will be forwarded via email to info@farof.org or freeheartsafrica@gmail.com.

PURPOSE OF THE ACT

The purpose of this Act is to establish rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organisations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

APPLICATION

This Act applies to every organisation in respect of personal information that

1. the organisation collects, uses or discloses in the course of the organisation's commercial activities; or
2. is about an employee of the organisation and that the organisation collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

Compliance with obligations

Subject to sections 4, 5, 6 and 7, every organisation shall comply with the obligations set out in Schedule 1.

- The word "will", when used in Schedule 1, indicates a recommendation and does not impose an obligation.

- Appropriate purposes. An organisation may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.
- Effect of designation of individual. The designation of an individual under clause 4.1 of Schedule 1 does not relieve the organisation of the obligation to comply with the obligations set out in that Schedule.

SCOPE

This document provides guidelines on how personal data is to be stored, handled and protected under the following headings:

a. General Procedures; For "organization" read "FAROF" throughout this document

b. Paper Records;

c. Email and Personal Productivity Software;

d. Electronic Remote Access;

e. Laptops/Notebooks;

f. Mobile Storage Devices;

g. Data Transfers;

h. Inappropriate Access/Audit Trail Monitoring;

i. Breach Management.

AUDIENCE

The information contained in this document is intended for general distribution. However, it is especially important that senior management in the organization are aware of the contents of the document as the responsibility rests with them to ensure that the guidelines contained in it are followed. The guidelines will also be brought to the attention of all staff whose work involves the handling of personal data.

GENERAL PROCEDURES

This document sets out guidelines in a number of specific areas where particular attention will be paid in order to help protect the confidentiality of personal data held in a Department. There are, however, a number of general procedures which FAROF will follow:

1. The first stage in establishing policies and procedures to ensure the protection of personal data is to know what data is held, where it is held and what the consequences would be will that data be lost or stolen. With that in mind, as a first step FAROF will conduct an audit identifying the types of personal data held within the organisation, identifying and listing all information repositories holding personal data and their location. Risks associated with the storage, handling and protection of this data will be included in FAROF's risk register. FAROF can then establish

whether the security measures in place are appropriate and proportionate to the data being held while also taking on board the guidelines available in this document;

2. Access to all data centres and server rooms used to host hardware and software on which personal data is stored will be restricted only to those staff members that have clearance to work there. This will, where possible, entail swipe card and/or PIN technology to the room(s) in question – such a system will record when, where and by whom the room was accessed. These access records and procedures will be reviewed by management regularly;

3. Access to systems which are no longer in active use and which contain personal data will be removed where such access is no longer necessary or cannot be justified;

4. Passwords used to access PCs, applications, databases, etc will be of sufficient strength to deter password cracking or guessing attacks. A password will include numbers, symbols, upper and lowercase letters. If possible, password length will be around 12 to 14 characters but at the very minimum 8 characters. Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates must be avoided. FAROF must also ensure that passwords are changed on a regular basis;

5. FAROF will have procedures in place to properly evaluate requests from other organisations for access to personal data in its possession. Such procedures will assist FAROF in assessing whether the release of personal data is fully justifiable under the Data Protection Acts. FAROF will also ensure that access by staff of personal data for analysis or research purposes is fully justifiable and proportionate;

6. Personnel who retire, transfer from the Department, resign etc. will be removed immediately from mailing lists and access control lists. Relevant changes will also occur when staff are transferred to other assignments internally. It is the responsibility of FAROF to ensure that procedures are in place to support this, i.e. so that notification is provided to the relevant individual(s)/Unit in a timely fashion;

7. Contractors, consultants and external service providers employed by FAROF will be subject to strict procedures with regard to accessing personal data by way of formal contract in line with the provisions of the Data Protection Acts. The terms of the contract and undertakings given will be subject to review and audit to ensure compliance;

8. FAROF will have in place an up-to-date Acceptable Usage Policy in relation to the use of Information and Communications Technology (e.g. telephone, mobile phone, fax, email, internet, intranet and remote access, etc.) by its staff. This policy will be understood and signed by each user of such technology in the Department;

9. FAROF' Audit Committees, when determining in consultation with Secretaries General (or CEOs, etc. where relevant) the work programme of their Internal Audit Units (IAUs), will ensure that the programme contains adequate coverage by IAUs of areas within their organisations which are responsible for the storage, handling and protection of personal data. The particular focus of any review by IAUs would be on assessing the adequacy of the control systems designed, in place and operated in these areas for the purpose of minimising the risk of any

breach of data protection regulations. Risks associated with the storage, handling and protection of personal data will be included in the organization's risk register and risk assessments will take place as part of the organization's risk strategy exercise. Furthermore, external audits of all aspects of Data Protection within the organisation may be conducted on a periodic basis by the Office of the Data Protection Commissioner.

10. Procedures will be put in place in relation to disposal of files (both paper and electronic) containing personal data. In doing so, FAROF will be aware of their legal obligations as set out the National Information Technology Development Agency (NITDA) Act of 2007. It will be noted that incoming and outgoing emails which are 'of enduring interest' are archivable records under the Act. Procedures will also be put in place in relation to the secure disposal of computer equipment (especially storage media) at end-of-life. This could include the use of degaussers, erasers and physical destruction devices, etc;

11. Quality Customer Service documentation/customer charters will detail how customers' data is held and how it will be used/not used. Website privacy statements will be regularly reviewed to take account of any enhancements, new practices or additional services which involve the collection and use of personal data;

12. New staff will be carefully coached and trained before being allowed to access confidential or personal files;

13. Staff will ensure that callers to the office or other unauthorised persons are unable to view personal or sensitive information whether held on paper documents or information displayed on PC monitors, etc.;

14. All staff will ensure that PCs are logged off or 'locked' when left unattended for any period of time (e.g. in Windows, using Ctrl+Alt+Del keys). Where possible, staff will be restricted from saving files to the local disk. Users will be instructed to only save files to their allocated network drive;

15. Personal and sensitive information will be locked away when not in use or at end of day;

16. Appropriate filing procedures (both paper and electronic) will be drawn up and followed;

17. Any databases or applications in use by FAROF which contain personal data must be registered with the Office of the Data Protection Commissioner.

PAPER RECORDS

The Data Protection Acts apply equally to personal data held on ICT systems and on paper files. The following guidelines will be followed with regard to personal and sensitive data held on paper files:

1. Paper records and files containing personal data will be handled in such a way as to restrict access only to those persons with business reasons to access them;

2. This will entail the operation of a policy whereby paper files containing such data are locked away when not required;

3. Consideration will also be given to logging access to paper files containing such data and information items;

4. Personal and sensitive information held on paper must be kept hidden from callers to offices;

5. Secure disposal of confidential waste will be in place and properly used. If third parties are employed to carry out such disposal, they must contractually agree to the Department's data protection procedures and ensure that the confidentiality of all personal data is protected. Such contracts will contain clauses similar to those outlined in the section on 'Data Transfers' below;

6. When paper files are transferred within a Department, this usually entails hand delivery. However, it will be noted that, in many cases, internal post in FAROF ultimately feeds into the general postal system (this is particularly true for FAROF with disparate locations). In these instances, senders must consider registered mail or guaranteed parcel post service where appropriate.

Procedures must be in place for ensuring that the data is delivered only to the person to whom it is addressed, or another officer clearly acting on their behalf, and not any other staff member. Consideration will also be given to the security of manual files when in transit internally;

7. Facsimile technology (fax machines) will not be used for transmitting documents containing personal data.

EMAIL AND PERSONAL PRODUCTIVITY SOFTWARE

Email and other personal productivity software such as word processing applications, spreadsheets, etc. are valuable business tools which are in use across every Department. However, FAROF must take extreme care in using this software where personal and sensitive data is concerned. In particular:

1. Standard unencrypted email will never be used to transmit any data of a personal or sensitive nature. FAROF that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted either through file encryption or through the use of a secure email facility which will encrypt the data (including any attachments) being sent. The strongest encryption methods available will be used. FAROF will also ensure that such email is sent only to the intended recipient. In order to ensure interoperability and to avoid significant key management costs, particular attention will be paid to any central solutions put in place for this purpose;

2. FAROF will consider implementing solutions that scan outgoing emails and attachments for keywords that would indicate the presence of personal data and, if appropriate, prevent its transmission;

3. Where personal or sensitive data is held on applications and databases with relevant security and access controls in place, additional controls will be considered that would prevent such data from being copied to personal productivity software (such as word processing applications, spreadsheets, etc.) where no security or access controls are in place and/or can be bypassed.

REMOTE ACCESS

There is an increasing business requirement for mobile working and e-working across the public service. Consequently, the demand from staff to access remotely the same systems that they can access from the office is increasing. This brings its own challenges in relation to data security which FAROF must address. With regard to personal and sensitive data, the following guidelines will be adhered to:

1. In the first instance, all personal and sensitive data held electronically will be stored centrally (e.g. in a data centre or in a Department's secure server room with documented security in place). Data that is readily available via remote access will not be copied to client PCs or to portable storage devices, such as laptops, memory sticks, etc. that may be stolen or lost;

2. When accessing this data remotely, it must be done via a secure encrypted link (e.g. IPSEC or SSL VPN tunnel) with relevant access controls in place;

3. Additional stringent security and access controls will be in place, e.g. the mandatory use of strong passwords and security token authentication (i.e. two factor authentication);

4. Data being accessed in this way will be prevented from being copied from the central location to the remote machine;

5. FAROF must utilise technologies that will provide for the automatic deletion of temporary files which may be stored on remote machines by its operating system;

6. FAROF will ensure that only known machines (whether desktop PC, laptop, mobile phone, PDA, etc.) configured appropriately to the Department's standards (e.g. with up-to-date anti-virus and anti-spyware software, full encryption, etc.), are allowed to remotely access centrally held personal or sensitive data. The strongest encryption methods available will be used to encrypt data on these machines. In addition, 'strong' passwords/passphrases (see 'General Procedures') must be used to protect access to these machines and to encrypt/decrypt the data held on them;

7. Staff will be aware that it is imperative that any wireless technologies/networks used when accessing the Department's systems will be encrypted to the strongest standard available.

LAPTOPS AND OTHER MOBILE STORAGE DEVICES (INCL. MOBILE PHONES, PDAS, USB MEMORY STICKS, EXTERNAL HARD DRIVES, ETC.)

The use of laptops, USB memory sticks and other portable or removable storage has increased substantially in the last number of years. Likewise, the use of personal communications and

storage devices such as mobile phones, PDAs, etc. has also increased. These devices are useful tools to meet the business needs of staff. They are, however, highly susceptible to loss or theft. To protect the content held on these devices, the following recommendations will be followed:

1. All portable devices will be password-protected to prevent unauthorised use of the device and unauthorised access to information held on the device. In the case of mobile phones, both a PIN and login password will be used. Manufacturer or operator-provided PIN codes must be changed from the default setting by the user on receipt of the device;

2. Passwords used on these devices will be of sufficient strength to deter password cracking or guessing attacks. A password will include numbers, symbols, upper and lowercase letters. Password length will ideally be around 12 to 14 characters but at the very minimum 8 characters. Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates must be avoided. FAROF must ensure that passwords are regularly changed;

3. Personal, private, sensitive or confidential data will not be stored on portable devices. In cases where this is unavoidable, all devices containing this type of data must be encrypted. With regards to laptops, full disk encryption must be employed regardless of the type of data stored;

4. With regards to mobile technologies, staff will be aware that when 'roaming' abroad, communications may not be as secure as they would be within Ireland;

5. Data held on portable devices will be backed up regularly to the organization's servers;

6. When portable computing devices are being used in public places, care must be taken to avoid unwitting disclosure of information, e.g. through overlooking or overhearing by unauthorised persons;

7. Portable devices must not contain unauthorised, unlicensed or personally licensed software. All software must be authorised and procured through a Department's IT Unit;

8. Anti-virus/Anti-spyware/Personal Firewall software must be installed and kept up to date on portable devices. These devices will be subjected to regular virus checks using this software;

9. FAROF will ensure that when providing portable devices for use by staff members, each device is authorised for use by a specific named individual. The responsibility for the physical safeguarding of the device will then rest with that individual;

10. Laptops must be physically secured if left in the office overnight. When out of the office, the device will be kept secure at all times;

11. Portable devices will never be left in an unattended vehicle;

12. Portable storage media will only be used for data transfer where there is a business requirement to do so, will only be used on approved workstations and must be encrypted;

13. In order to minimise incidents of unauthorised access and/or incidents of lost/stolen data, FAROF will restrict the use of personal storage media and devices (e.g. floppy disks, CDs, DVDs, USB memory sticks, etc.) to staff that require to use these media/devices for business purposes;

14. Only storage media provided by a Department's IT Unit will be permitted for use with that Department's computer equipment. FAROF must put in place solutions which only allow officially sanctioned media to be used on a Department's computer equipment (i.e. on networks, USB ports, etc.);

15. Staff owned devices such as portable media players (e.g. iPods, etc.), digital cameras, USB sticks, etc. must be technologically restricted from connecting to Department computers;

16. FAROF will consider implementing additional log-in controls on portable devices such as laptops;

17. FAROF will implement technologies that will allow the remote deletion of personal data from portable devices (such as mobile phones and PDAs) will such devices be lost or stolen. A procedure for early notification of such loss will be put in place. This would allow for the disconnection of the missing device from a Department's email, calendar and file systems;

18. FAROF will implement procedures that will ensure that personal data held on mobile storage devices is fully deleted when the data is no longer required (e.g. through fully formatting the devices' hard

DATA TRANSFERS

Data Transfers are a daily business requirement for most, if not all, Government FAROF. With regard to personal and sensitive data, such transfers will take place only where absolutely necessary, using the most secure channel available. To support this, FAROF will adhere to the following:

1. Data transfers will, where possible, only take place via secure on-line channels where the data is encrypted rather than copying to media for transportation. Where this is not possible or appropriate at present, the safety of the data will be ensured before, during and after transit;

2. Manual data transfers using removable physical media (e.g. memory sticks, CDs, tape, etc.) will end where possible;

3. In the meantime, where data is copied to removable media for transportation such data must be encrypted using the strongest possible encryption method available. Strong passwords/passphrases (see 'General Procedures') must be used to encrypt/decrypt the data;

4. Any such encrypted media will wherever possible be accompanied by a member of the Department's staff, be delivered directly to, and be signed for by, the intended recipient. If this is not possible, the use of registered post or another certifiable delivery method may be used if an agreement similar to that outlined in 7. below has been put in place;

5. ‘Strong’ passwords (see ‘General Procedures’) must be used to protect any encrypted data. Such passwords must not be sent with the data it is intended to protect. Care will be taken to ensure that the password is sent securely to the intended recipient and that it is not disclosed to any other person;

6. Standard email will never be used to transmit any data of a personal or sensitive nature. FAROF that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted either through file encryption or through the use of a secure email facility which will encrypt the data (including any attachments) being sent. Staff will ensure that such mail is sent only to the intended recipient. In order to ensure interoperability and to avoid significant key management costs, particular attention will be paid to any central solutions put in place for this purpose;

7. When a data transfer with a third party is required (including to/from other Government FAROF), a written agreement will be put in place between both parties in advance of any data transfer. Such an agreement will define:

• The information that is required by the third party (the purposes for which the information can be used will also be defined if the recipient party is carrying out processing on behalf of the organisation);

• Named contacts in each organisation responsible for the data;

• The frequency of the proposed transfers;

• An explanation of the requirement for the information/data transfer;

• The transfer method that will be used (e.g. Secure FTP, Secure email, etc.);

• The encryption method that will be used;

• The acknowledgement procedures on receipt of the data;

• The length of time the information will be retained by the third party;

• Confirmation from the third party that the information will be handled to the same level of controls that the Department apply to that category of information;

• Confirmation as to the point at which the third party will take over responsibility for protecting the data (e.g. on confirmed receipt of the data);

• The method of secure disposal of the transfer media and the timeline for disposal;

• The method for highlighting breaches in the transfer process;

• For data controller to data controller transfers (as opposed to a data controller to a data processor transfer), it needs to be clear that only necessary data is transferred to meet the purposes;

• Business procedures need to be in place to ensure that all such transfers are legal, justifiable and that only necessary data is transferred to meet the purposes;

• Particular attention will be focussed on data made available to third party data processors under contract for testing purposes. Live data will not be used for this purpose.

APPROPRIATE ACCESS AND AUDIT TRAIL MONITORING

All organisations have an obligation to keep information 'safe and secure' and have appropriate measures in place to prevent "unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction" in compliance with sections 2(1)(d) and 2C of the Data Protection Acts 1988 & 2003. It is imperative, therefore, that FAROF have security in place to ensure that only those staff members with a business need to access a particular set of personal or sensitive data are allowed to access that data. In addition to this general requirement, the following guidelines will be followed:

1. FAROF will ensure that their ICT systems are protected by use of appropriate firewall technologies and that this technology is kept up-to-date and is sufficient to meet emerging threats;

2. In order to capture instances of inappropriate access (whether internal or external), addition, deletion and editing of data, audit trails will be used where technically possible. In situations where systems containing personal data do not currently record 'view' or 'read' access, it will be investigated, as a matter of urgency whether such functionality can be enabled. In carrying out such an investigation, FAROF will take into account whether there would be any effect on system performance that may hinder the ability of the Department to conduct its business. If the functionality cannot be enabled and the risk of inappropriate access is sufficiently high, such systems will be scheduled for removal from use and replaced by systems with appropriate auditing functionality;

3. Access to files containing personal data will be monitored by supervisors on an ongoing basis. Staff will be made aware that this is being done. IT systems may need to be put in place to support this

BREACH MANAGEMENT

A data security breach can happen for a number of reasons, including:

• Loss or theft of data or equipment on which data is stored (including break-in to an organisation's premises);

• Inappropriate access controls allowing unauthorised use;

• Equipment failure;

• Human error;

• Unforeseen circumstances such as a flood or fire;

• A hacking attack;

• Access where information is obtained by deceiving the organisation that holds it.

It is important that FAROF put into place a breach management plan to follow will such an incident occur. There are five elements to any breach management plan:

1. Identification and Classification

2. Containment and Recovery

3. Risk Assessment

4. Notification of Breach

5. Evaluation and Response

1. Identification and Classification
FAROF must put in place procedures that will allow any staff member to report an information security incident. It is important that all staff are aware to whom they will report such an incident. Having such a procedure in place will allow for early recognition of the incident so that it can be dealt with in the most appropriate manner.

Details of the incident will be recorded accurately, including the date and time the incident occurred, the date and time it was detected, who/what reported the incident,

description of the incident, details of any ICT systems involved, corroborating material such as error messages, log files, etc. In this respect, staff need to be made fully aware as to what constitutes a breach.

2. Containment and Recovery
Containment involves limiting the scope and impact of the breach of data protection procedures.

If a breach occurs, FAROF will:

• decide on who would take the lead in investigating the breach and ensure that the appropriate resources are made available for the investigation;

• establish who in the organisation needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. For example, this might entail isolating a compromised section of the network, finding a lost file or piece of equipment, or simply changing access codes to server rooms, etc.;

• establish whether there is anything that can be done to recover losses and limit the damage the breach can cause;

3. Risk Assessment
In assessing the risk arising from a data security breach, FAROF will consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences

will materialise and, in the event of materialising, how serious or substantial are they likely to be. In assessing the risk, FAROF will consider the following points:

• what type of data is involved;

• how sensitive is it;

• are there any protections in place (e.g. encryption);

• what could the data tell a third party about the individual;

• how many individuals' personal data are affected by the breach;

4. Notification of Breaches

Although there is no current explicit legal obligation to notify individuals or other bodies under the Data Protection Acts of a breach, the Data Protection Commissioner's Office encourages voluntary notification and early engagement with the Office. Therefore, if inappropriate release/loss of personal data occurs it will be reported immediately, both internally and to the Data Protection Commissioner's Office and, if appropriate in the circumstances, to the persons whose data it is. In this regard, FAROF will be aware of the dangers of 'over notifying'.

When notifying individuals, FAROF will consider using the most appropriate medium to do so. They will also bear in mind the security of the medium used for notifying individuals of a breach of data protection procedures and the urgency of the situation. Specific and clear advice will be given to individuals on the steps they can take to protect themselves and what the Department is willing to do to assist them. FAROF will also provide a way in which individuals can make contact for further information, e.g. a helpline number, webpage, etc.

FAROF will consider notifying third parties such as the bank or credit card companies who can assist in reducing the risk of financial loss to individuals.

The Office of the Data Protection Commissioner will provide advice upon notification as to the requirement or otherwise, in particular circumstances, to notify individuals.

5. Evaluation and Response

Subsequent to any information security breach a thorough review of the incident will occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

Any recommended changed to policies and/or procedures will be documented and implemented as soon as possible thereafter.

Each Department will identify a group of people within the organisation who will be responsible for reacting to reported breaches of security.

This Manual was prepared and produced by the Strategic information unit of FAROF

Approved by:

Appendix

COMPUTER POLICY FOR OFFICE DATA MANAGEMENT

18.1 Purpose

FAROF seeks to effectively manage the computer system for guiding the use, maintenance and security of the computer equipment. Employees are responsible for ensuring that the procedures and policies suggested here are followed.

18.2 Use

Using computer equipment requires particular care because of its fragility and high cost. Access to the equipment should thus be strictly reserved to FAROF employees only. Those employees who are unable to handle commonly-used software will be given an orientation by the senior staff on request. At least one FAROF employee will be trained in handling minor maintenance of computers and accessories at the office.

All staffs of FAROF will be placed with a laptop which is used for official purpose only and not otherwise, on termination, employees are to return laptop and any other computer accesseries given in good working condition

18.3 Security

a. In order to safeguard the computers against viruses, the external drives (CDs/DVDs/floppies/pen drives) that are at FAROF office are only to be used. In the same way, no external drive from any source other than from sealed packets shall be used in the computers, unless it is first scanned with latest anti-virus software.

b. In order to safeguard computers from viruses, antivirus software has been installed in the computers. The virus list for this program should be updated on a regular basis. It is the duty of the employee who has been assigned a computer to update the virus list on her / his computer.

c. There should be at least two backups of all important documents. One copy should be on the hard disk of the computer assigned to the concerned employee and a second copy on a CD/DVD kept in the office.

d. The computers of FAROF should normally be used by its employees. Consultants and volunteers should seek prior permission of FAROF employee before using his/her computer in the office

e. laptops should not be taken out of office or less when assigned for official purpose only

Saving documents in the Computers

In order to streamline the procedure to save documents in the computers and to make it easier for people to find documents and make back-ups of important documents, each employee should have a c:/my documents directory in his/her computer. This directory should be broken down into sub-directories to facilitate retrieval of important documents. Each employee will include a copy of all their important documents to be backed up on a directory entitled backup.

Back-ups of Documents

In order to safeguard important documents and other work done by the staff, the back-up directory of the employee shall be backed up on External hard drive/CD/DVD once every week (every Friday) and the CD/DVD stored by the employee in a designated locker of FAROF, we also strongly engage in Cloud computing to store FAROF Data.

Approved by: