MAZE LONG KESH

Development Corporation

Security Policy & Procedures

Author:
Version: 5.0
Date: 15 August 2019
TRIM Ref: DF1/13/714272[v5]

This document explains the Maze Long Kesh Development Corporation (MLKDC) security policy. It deals with records and information security, and IT security. The majority of MLKDC's records and information are now held electronically so IT security is particularly important.

You have a personal responsibility to maintain security, especially of the records and information used by the MLKDC.

1. SECURITY RESPONSIBILITIES

The Chief Executive (CE) is responsible for security matters in MLKDC. In Civil Service terms, although MLKDC is an Executive Non Departmental Public Body (NDPB), the CE is the Departmental Security Officer (DSO) who oversees all matters relating to security within the MLKDC.

The DSO answers to the MLKDC Board. MLKDC is an NDPB of The Executive Office (TEO) so ultimately, MLKDC security is the responsibility of TEO. TEO should be consulted on all matters that affect security policy.

2. PERSONAL PROPERTY

In most circumstances, MLKDC cannot accept responsibility for your personal property lost or damaged during the course of employment. It is your responsibility to safeguard personal belongings. You should not leave personal property unsecured in the office overnight or unattended during office hours.

Lock away in cabinets or cupboards or take with you your personal property, cash or valuables whenever you are away from your desk.

You should report faulty or broken furniture locks to the Premises Officer.

Similarly you should report immediately to the Director of Finance and Corporate Services any incidents of theft.

3. PHYSICAL SECURITY

The Development Officer is responsible for the supervision of security measures at MLKDC. You should make sure that you know what to do in case of fire, a bomb alert or other emergency. See the MLKDC Emergency Evacuation Procedures (Ref. FI1/17/396832)) for more information.

In the unlikely event that you receive a suspicious letter or package, see Dealing With Suspicious Mail on the DoF Intranet.

4. DOCUMENT AND INFORMATION SECURITY

You are responsible for document and information security, including the security of documents from other organisations or departments that you may use or have access to in the course of your work.

4.1 Document and Information Security Principles

Some of our records and information are likely to be commercially or politically sensitive, which requires you to be vigilant in handling them. You should be particularly careful of personal data.

You should always.

a) Store electronic records in HPRM – see Section 5 below.

b) Store paper records in the locked furniture supplied.

c) Do not send large amounts of personal or other information by mail (e.g. mailing a database on a CD) unless it is securely encrypted. You should use a secure, signed for postal / courier service; and you must ask the CE first.

d) Lock away documents, portable devices, equipment, etc. Do not leave things lying around.

e) Operate a clear desk policy in the office – see MLKDC's End of Day Procedures DF1/16/133663).

f) Always collect printing and photocopies of sensitive material. Do not leave copies lying around.

g) If you handle protectively marked records, consult the CE or the Information Manager – see Section 4.3 below.

h) Outside the office, keep sensitive records with you at all times.

i) Outside the office, electronic information must be encrypted on laptops or USB sticks – see Section 5 below.

j) Carry sensitive papers in an opaque container e.g. a briefcase or card folder, not in a clear plastic folder.

k) Away from the office keep things locked and out of sight in the car boot when in transit. When working at home keep them out of view and secure. Do not leave laptops, documents, etc. overnight in your car. Keep them with you.

l) Protect personal data from loss or compromise – see MLKDC's GDPR & Data Protection Policy & Procedures (FI1/18/628798) for more guidance.

All the above will prevent inadvertent loss of information or unauthorised access to it.

4.2 Storage of Records

All MLKDC records should be stored in HPRM, the Electronic Documents and Records Management System (EDRMS) used by MLKDC. Very few if any records should be stored in paper format. The records management system, the lockable cupboards and the network used by MLKDC are accepted by TEO for handling documents up to the level of OFFICIAL.

4.3 Protective Markings

You should be aware of the Government Protective Marking System. The government protective markings are TOP SECRET, SECRET and OFFICIAL.

The MLKDC Document Classification Policy (DF1/16/283708) sets out the methodology of how information is handled and protected against the risk of unauthorised disclosure. You may receive protectively marked documents from Government Departments so you need to respect their security levels.

All of MLKDC's containers in HPRM have their access restricted at a minimum to MLKDC and the Strategic Investment Board (SIB) staff only (SIB supply staff to MLKDC). This means that no one outside of MLKDC, apart from the system administrators, should be able to see MLKDC records. Some containers (e.g. personnel or finance records) will be further restricted.

Be particularly vigilant when emailing using a group email distribution list. The group may contain non NICS email addresses: i.e. the email will go out to some recipients via the Internet.

4.4 Exchanging Large Files with Third Parties

You must be vigilant when sending, receiving or exchanging large files or attachments over the Internet. In general, IT Security Policies prevent you or restrict you doing this e.g. online file stores are blocked. However, see paragraph 4.3 above. In particular:

- **You must not send security marked documents via the Internet** (i.e. anything marked OFFICIAL or above – see Section 5.2.)
- **You must not send commercially (or otherwise) sensitive material via the Internet.**

If you have to send sensitive / restricted material, either use the NICS internal systems (e.g. email and HPRM links) or, at a minimum, use a secure, signed-for postal / courier service where appropriate (e.g. for personal data).

4.4.1 Email

For sending emails, the individual email size limits are set to 10 MB for external emails and 30 MB for internal emails. However, if an email is blocked from being sent because of size you will not receive a warning. If you send a large email you should confirm the next day that the intended recipients did receive it.

There is at least a larger size limit on emails that you receive. However, the practical issue is that it takes only a few large emails to lock your Outlook by exceeding the size restrictions for mailboxes.

4.5 More Information on Information Security

More information on MLKDC's record and information policies and procedures can be found in the MLKDC Records and Information Management Policy (Ref. DF1/13/690810).

5. IT Security

MLKDC's IT services are supplied by IT Assist. The purpose of IT security is to ensure:

- **Confidentiality** – Access to information is restricted to authorised personnel.
- **Integrity** – Information held is accurate and can only be altered by authorised personnel.
- **Availability** – IT systems are available as and when required by you.

5.1 NICS Laptop Security Policy

The Northern Ireland Civil Service (NICS) Laptop Security Policy applies to MLKDC. The purpose of the policy is to ensure that staff are fully aware of the requisite security needed to protect a laptop, be it in a secure NICS office environment or any other location.

MLKDC staff are provided with laptops by IT Assist. Therefore you must be familiar with this policy. Some key points are:

a) Information stored on a laptop should be kept to the absolute minimum required for effective working.

b) All laptops should now be encrypted (i.e. require the use of a username and password to start up).

c) The username and password must never be stored or carried in the same bag as the laptop.

d) Laptops must not be left in an unattended car and when in transit they must be locked in the boot.

e) When a laptop is removed from a secure location it must, whenever practical, be kept out of sight when not in use.

f) If a laptop or logon details are lost or stolen you must inform IT Assist and the IT Security Officer immediately – see MLKDC Procedures on Loss or Theft of Data or ICT Devices (DF1/13/714279).

g) Laptops and USBs are encrypted devices so losses must be reported to DoF and to Comsec Incident Notification, Reporting and Alerting Scheme (CINRAS) by TEO IT Security Officer (ITSO) who is also MLKDC's ITSO. The user will be required to complete a detailed form explaining the circumstances around the loss. In addition, MLKDC has taken the decision that no personal or sensitive data is to be stored on a laptop.

h) During office hours laptops should not be left unattended unless firmly secured by the cable lock provided.

i) Laptops must be properly closed down when not in use and secured in a suitable locked cabinet. Cable locks are not secure out of hours.

j) Encrypted devices **must not** be taken outside the UK without the CE's approval. The CE is responsible to TEO for security.

k) Note that a laptop must be connected to the network at least once every month to ensure that security, anti-virus and other updates are deployed or updated as needed.

5.2 IT Security Principles

You should always be doing the following.

RULE		WHY
PASSWORDS		
Use complex passwords	For your laptop and any secure USB sticks (that you use. A complex password is long (more than eight characters), mixes upper and lower case letters, contains numbers, and ideally contains symbol characters (e.g. "£", "^", etc.).	Stops unauthorised access.
Keep your passwords safe	Do not write them down and in particular do not keep a written down password with the device.	Stops unauthorised access.
Do not share your password	Do not share your password with anyone, even your manager. If you have to (e.g. where IT Assist need access to your PC) change your password immediately afterwards.	Stops unauthorised access.
RECORDS AND INFORMATION		
Store electronic records in HPRM	HPRM is secure and makes it easier to manage MLKDC records.	Stops unauthorised access.
Avoid copying databases, etc. to external media: e.g. CDs, DVDs, USB sticks, etc.	Where possible use links to HPRM, which controls and audits who accesses information. If absolutely necessary, make sure data is securely encrypted (e.g. by using an encrypted USB stick).	Reduces the chances for significant data losses and security breaches.
Restrict individual records	Restrict individual records only if appropriate. You can amend the security access of any record but exercise care in doing this. For the vast majority of records the default MLKDC container security setting is fine.	Stops unauthorised access.

EQUIPMENT		
Dispose of IT equipment properly	For example, laptops must be handed back to IT Assist so that they can securely wipe the hard disks (as well as disposing of them in accordance with environmental legislation).	Stops inadvertent security breaches or losses of information.
Switch off or lock PCs, etc.	Equipment should be switched off at night and if you leave your desk. Lock your PC – "Windows Key + L" is the shortcut. (Alternatively, "Ctrl+Alt+Del" and select "Lock Computer"). Lock laptops away.	Stops unauthorised people gaining access.
Keep portable equipment with you.	Do not leave your laptop, Blackberry or your USB stick lying around, especially when out of the office. You **must** lock them away outside working hours.	Stops thieves and unauthorised access.
Use a Kensington Lock	Use a Kensington Lock to secure your laptop while working away from the office.	Stops thieves and unauthorised access.
Only connect authorised equipment	Only connect authorised equipment to office laptops or the network.	Stops the introduction of viruses or inadvertently compromising the network security for everybody.
SOFTWARE		
Only install authorised or approved software	If you need software, speak to the CE. Only IT Assist can install software, for which they will require a service request that only the CE can authorise and the Information Manager can create.	Stops the introduction of viruses or inadvertently compromising the network security for everybody.
Respect copyright	You must not copy licensed software.	Stops MLKDC being sued or otherwise embarrassed.
THE INTERNET		
Use the Internet sensibly	Internet access is provided as a work tool. You are allowed reasonable access for private use but this should be in your own time: e.g. before work or in your lunch break.	You are paid to work not play.

Avoid dubious websites.	This goes beyond the obvious malefactors. The network filters prevent access to many sites but they cannot block all of them. Exercise common sense over what you view.	Stops the introduction of viruses or inadvertently compromising the network security for everybody. Protects MLKDC's reputation (e.g. would MLKDC be happy if a newspaper knew you were visiting a particular site?
Be aware that Internet access is logged.	You do not want to do anything you should not.	Enables IT to detect security issues.
Avoid adverse comment on MLKDC	For example, do not make comments on bulletin boards, social networking sites and the like.	Avoid embarrassing yourself and MLKDC, and avoid harming MLKDC's reputation.
EMAIL		
Avoid adverse comment on MLKDC	Your email may have a limited address list but anyone can forward it to the world.	Avoid embarrassing yourself and MLKDC, and avoid harming MLKDC's reputation.
Be careful what you email	Internal addresses on Outlook are on a secure RESTRICTED network. However, anything else goes out via the Internet. Potentially it can be seen by anyone in the world so think about what you send this way.	Stops inadvertent security breaches or losses of information. Avoid embarrassing yourself and MLKDC, and avoid harming MLKDC's reputation. Would you be happy if what you said was published in a newspaper tomorrow?
Send HPRM links	Send HPRM links Instead of original documents where possible.	Stops inadvertent security breaches or losses of information. HPRM controls and audits who accesses information.

Do not email large amounts of information	Ideally, send a TRIM link instead. If you cannot then, for example, do not send large amounts of personal or other sensitive information by email unless it is within the NICS email network.	Stops inadvertent security breaches or losses of information.
REPORT SECURITY BREACHES IMMEDIATELY		
	If you lose a piece of equipment or it is stolen, report it to the CE and IT Assist as soon as possible. Follow the procedure in DF1/13/714279 MLKDC Procedures on Loss or Theft of Data or ICT Devices.	Enables IT Assist to take action to prevent further loss: e.g. they could disable a stolen Blackberry.
	If you think sensitive information has been compromised, report it to the CE as soon as possible	Allows any damage limitation exercise to get underway as soon as possible.

6. SECURITY FURNITURE

You should be provided with a secure cabinet drawer or cupboard in which you can lock papers, equipment and personal possessions. If you need more storage space, speak to the Premises Officer. However, MLKDC's information management policy is to minimise paper storage. Documents and other records should be stored electronically as far as possible.

The security furniture is supplied by the DoF and meets the minimum document and IT security standards specified by TEO. This means that documents up to the level of OFFICIAL can be stored in them.