Iż-Żejtun Local Council

Information Security Policy

(including Clean Desk Policy, Anti-Virus Guidelines and Cyber Security Approach)

CONTENTS

1 Introduction 3
2 Policy Compliance 4
3 Legal Aspects 4
4 Responsibilities 4
PART 1 - KEEPING INFORMATION SECURE 6
5 Data Protection by Design and Default 6
6 Data Breaches and Information Security Incidents 6
7 Access control 7
8 Security of Equipment 8
9 Security and Storage of Information 9
10 Clear Desk Policy 10
11 Posting or Emailing Information 10
12 Redacting 11
13 Sharing and Disclosing Information 12
14 Retention and Disposal of Information 12
15 Vacating Premises or Disposing of Equipment 13
PART 2 – ICT SECURITY 13
16 Cloud Storage Solutions 13
17 Systems Development 14
18 Network Security 14
19 Risks from Viruses 14
20 Cyber Security 14
21 Access Control to Secure Areas 14
22 Security of Third Party Access 15
23 Data Back-up 16
24 Equipment, Media and Data Disposal 16
25 Software 17
26 Use of Removable Media 18
27 Timeout Procedures 18
28 System Documentation 18
29 Contact information regarding data protection 19
30. APPROVALS AND SIGN OFFS 19
31. VERSION CONTROL 20
APPENDIX 1 - Anti-Virus Guidelines 21
APPENDIX 2 - Cyber Security Approach 25

1 Introduction

The General Data Protection Regulation (GDPR) defines that all public authorities must adhere to the regulations thereof and Member State data protection legislation.

In terms of the Local Government Act (CAP 363) of the Laws of Malta, the Iż-Żejtun Local Council (hereafter referred to as the 'Local Council') is a statutory Local government authority, hence a public authority under the GDPR, having a distinct legal personality and capable of entering into contracts, of suing and being sued, and of doing all such things and entering into such transactions as are incidental or conducive to the exercise and performance of its functions as are allowed under the Act. The full and updated version of the Act can be reviewed from:

http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8833

All information held by the Council, in all formats, represents an extremely valuable asset and, therefore, must be used and stored in a secure manner.

This Policy is in two parts, the first outlines security procedures covering all aspects of processing information. The second part covers security of IT systems.

The Policy must be read in conjunction with other policies, including:

- Data Protection Policy
- Security Incident and Personal Data Breach Policy

The Policy applies to all Members and employees of the Council, both permanent and temporary. It also applies to contractors, business partners and visitors, not employed by the Council but engaged to work with or who have access to Council information, (e.g. computer maintenance contractors) and in respect of any externally hosted computer systems.

The Policy applies to all locations from which Council systems are accessed (including home use). Where there are links to enable non-Council organisations to have access to Council information, officers must confirm the security policies they operate meet the Council's security requirements. A copy of any relevant third-party security policy should be obtained and retained with the contract or agreement.

Suitable third-party processing agreements must be in place before any third party is allowed access to personal information for which the Council is responsible.

2 Policy Compliance

2.1 The Executive Secretary should ensure all staff are aware of and understand the content of this policy.

2.2 If any user is found to have breached this policy, they could be subject disciplinary action. Serious breaches of this policy could be regarded as gross misconduct.

3 Legal Aspects

3.1 Some aspects of information security are governed by legislation, the most notable European and the Laws of Malta are listed below:

- General Data Protection Regulation (GDPR)
- The Data Protection Act (CAP 586)
- The Local Government Act (CAP 363)
- The Copyright Act (CAP 415)
- The Civil Code (CAP 16)

4 Responsibilities

4.1 The Executive Secretary must:

- be aware of information or portable ICT equipment which is removed from the civic offices for the purpose of site visits or home working and ensure staff are aware of the security requirements detailed in section 8, below

- ensure all staff, whether permanent or temporary, are instructed in their security responsibilities

- ensure staff using computer systems/media are trained in their use

- determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status

- ensure staff are unable to gain unauthorised access to Council IT systems or manual data

- implement procedures to minimise the Council's exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review or staff rotation in

critical susceptible areas

- ensure current documentation is maintained for all critical job functions to ensure continuity in the event of relevant staff being unavailable

- ensure that the relevant system adminstrators are advised immediately about staff changes affecting computer access (e.g. job function changes leaving business unit or organisation) so that passwords may be withdrawn or changed as appropriate

- ensure that all contractors undertaking work for the Council have signed confidentiality (non-disclosure) undertakings

- ensure the Council's Clear Desk Policy is enforced, particularly in relation to confidential or personal information. The Clear Desk Policy can be found in Section 10 below.

- ensure information held is accurate, up to date, and retained, in line with Council retention and disposal

- ensure relevant staff are aware of and comply with any restrictions specific to their role or service area.

4.2 Members and Staff are responsible for:

- ensuring that no breaches of information security result from their actions.

- reporting any breach, or suspected breach of security without delay. Further details can be found in the Security and Personal Data Breach Policy

- ensuring information, they have access to remains secure. The level of security will depend on the sensitivity of the information and any risks which may arise from its loss.

- ensuring they are aware of and comply with any restrictions specific to their role or service area.

4.3 All Members of staff should be aware of the confidentiality clauses in their contract of employment.

4.4 Advice and guidance on information security can be provided by the Data Protection Officer and, in relation to IT security, the IT Service Provider.

PART 1 - KEEPING INFORMATION SECURE

5 Data Protection by Design and Default

5.1 The General Data Protection Regulation (GDPR) requires that organisations put in place appropriate technical and organisational principles and safeguard individual rights. This is known as 'data protection by design and by default'. This means that the Council has to integrate data protection into processing activities and business practices, from the design stage right through the lifecycle.

5.2 The Council will, therefore, ensure that privacy and data protection is a key consideration in everything it does. As part of this the Council will:

- consider data protection issues as part of the design and implementation of systems, services, products and business practices;
- make data protection an essential component of the core functionality of our processing systems and services
- anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals
- only process the personal data that we need for our purpose(s) and that we only use the data for those purposes

5.3 Core privacy considerations should be incorporated into existing project management and risk management methodologies and policies to ensure:

- Potential problems are identified at an early stage
- Increased awareness of privacy and data protection
- Legal obligations are met and data breaches are minimised
- Actions are less likely to be privacy intrusive and have a negative impact on individuals

5.4 Data Protection Impact Assessments (DPIAs) are an integral part of taking a privacy by design approach.

6 Data Breaches and Information Security Incidents

6.1 The Council has a duty to ensure that all personal information is processed in compliance with the principles set out in the GDPR. It is ultimately the responsibility of the Executive Secretary, as Data Controller, to ensure that their service areas comply with that duty and that suitable procedures are in place for staff to follow when dealing with personal information.

6.2 Staff should be aware of requirements in relation to identifying and reporting security incidents and personal data breaches, as set out in the policy.

7 Access control

7.1 Staff, Members and contractors should only access systems for which they are authorised. Under the Civil Code (CAP 14) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

7.2 Formal procedures will be used to control access to systems. An authorised member of staff must raise an IT Service Request for each application for access. Access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Managers must ensure they advise IT of any changes requiring such modification /removal.

7.3 Staff, Members and contractors must comply with the Council's policy in relation to passwords.

7.4 The Executive Secretary must ensure that passwords to local systems are removed or changed to deny access.

7.5 Where appropriate, staff working out notice are assigned to non-sensitive tasks or are appropriately monitored.

7.6 Particular attention should be paid to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals & documents.

7.7 Once an employee has left, it can be impossible to enforce security disciplines, even though legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

7.8 The Executive Secretary must delete or disable all identification codes and passwords relating to members of staff who leave the employment of the Council on their last working day and that all PC files of continuing interest to the business of the Council are transferred to another user before the member of staff leaves.

7.9 The Executive Secretary must ensure that staff leaving the Council's employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving, make this likely then access rights should be restricted to avoid damage to Council information and equipment.

7.10 All visitors and temporary staff should have official identification issued by the Council. If temporary passwords need to be issued to allow access to confidential systems, these need to be disabled when the visitor or temporary staff has left. Visitors and temporary staff should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

7.11 There is a requirement for system administrators to have a procedure in place for the secure control of contractors called upon to maintain and support computing equipment and software. The contractor may be on site or working remotely via a communications link. IT Services will advise on the most suitable control.

7.12 Physical security to all office areas is to be provided through an access control system.

8 Security of Equipment

8.1 Portable computers, such as laptops and tablets, must have appropriate access protection, for example passwords and encryption, and must not be left unattended in public places.

8.2 Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when you are leaving the office.

8.3 Due to the high incidence of car thefts laptops or other portable equipment must **never** be left unattended in cars or taken into vulnerable areas.

8.4 Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off Council property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly.

8.5 Staff working from home must ensure appropriate security is in place to protect Council equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring Council equipment and information is kept out of sight.

8.6 Council issued equipment must not be used by non-Council staff.

8.7 Users of this equipment must pay particular attention to the protection of personal data and commercially sensitive data. The use of a password to start work with the computer when it is switched on, known as a 'power on' password, is mandatory and all sensitive files must be password protected if encrypting the data is not technically possible. The new user will refer to the instruction book to learn how to apply these passwords or may make arrangements for basic training in the use of a portable computer.

8.8 Users of portable equipment away from Council premises should check their car and home insurance policies for their level of cover in the event of equipment being stolen or damaged

and take appropriate precautions to minimise risk of theft or damage.

8.9 Staff and Members who use portable computers belonging to the Council must use them solely for business purposes.

9 Security and Storage of Information

9.1 All information, whether electronic or manual, must be stored in a secure manner, appropriate to its sensitivity. It is for each service area to determine the sensitivity of the information held and the relevant storage appropriate to that information. Suitable storage and security should include:

- Paper files stored in lockable cupboards or drawers
- Laptops stored in lockable cupboards or drawers
- Electronic files password protected or encrypted
- Restricted access to ICT systems
- Computer screens to be 'locked' whenever staff leave their desk
- Removable media to be kept in lockable cupboards or drawers and information deleted when no longer required
- Paper files removed from the office (for site visits or when working from home) to be kept secure at all times and not left in plain sight in unattended vehicles or premises
- Laptops must **never** be left in unattended vehicles
- It is advisable that paper files containing personal or sensitive data are kept separate from laptops, particularly when working from home
- At no time should sensitive, confidential or personal information be stored on a portable unit's hard drive. Access to this type of information must always be through the Council's network.
- To preserve the integrity of data, frequent transfers must be maintained between portable units and the main Council computer system.

- Staff should be aware of the position of their computer screens and take all necessary steps to prevent members of the public or visitors from being able to view the content of computers or hard copy information

10 Clear Desk Policy

10.1 Employees are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into desk drawers and cupboards as appropriate.

10.2 Although security measures are might be in place to ensure only authorised access to office areas, employees should ensure that documents, particularly of a confidential nature are not left lying around.

10.3 Employees must ensure that documents are carefully stored. When properly implemented, this clear desk policy also improves efficiency as documents can be retrieved more easily.

11 Posting or Emailing Information

11.1 If information is particularly sensitive or confidential the most secure method of transmission must be selected. The following procedures should be adopted as appropriate, depending on the sensitivity of the information.

11.2 One must consider the risk of harm or distress that could be caused to the customer if the information was lost or sent to another person, then look at the most appropriate way of sending the information to the recipient.

11.3 It is important that only the minimum amount of personal or sensitive information is sent, by whichever method is chosen.

11.4 Sending information by email:

- Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes

- If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the auto complete list. Both of these options can be found in Outlook under 'file', 'options' and 'mail'

- Take care when replying 'to all' – do you know who all recipients are and do they all need to receive the information you are sending

- If emailing sensitive information, password protect any attachments. Use a different method to communicate the password eg telephone call, messenger or text

- Consider the use of secure email where this is available or use drop off and encrypt the document

- Person identifiable data files **must not** be sent via email to a user's personal mailbox. Staff working from home should only access information via the Council's network.

11.5 Sending information by post:

- Check that the address is correct

- Ensure only the relevant information is in the envelope and that someone else's letter hasn't been included in error

- If the information is particularly sensitive or confidential, discuss the most secure method of delivery with the Executive Secretary including courier services and ensure that they are GDPR complaint.

11.6 Printing and Photocopying:

- When printing or photocopying multiple documents, ensure you separate them when you return to your desk.

- If the copier jams please remove all documents – if the copier remains jammed report it, but leave your contact details on the copier so that once it has been fixed any remaining copying can be returned to you and shredded immediately.

- Make sure your entire document has copied or printed – check that the copier has not run out of paper. This is particularly important when copying or printing large documents. Please bear in mind the printer will sometimes pause in the middle of a large print run.

- Do not leave the printer unattended when you're using it – someone else may come along and pick up your printing by mistake

12 Redacting

12.1 If it is necessary to redact information, either before sending it out or posting it onto the website, ensure a suitable and permanent redaction method is used.

12.2 The use of black marker pen is **not** a suitable method of redaction.

12.3 It is not advisable to change the colour of text (eg white text on a white background) or use text boxes to cover text as these can be removed from electronic documents. However, if this is the only option, once redacted the document should be printed and then scanned as a PDF before being sent.

13 Sharing and Disclosing Information

13.1 When disclosing personal or sensitive information to customers, particularly over the phone or in person, verification of their identity is a necessity.

13.2 If such data is not the property of the Council, information shall only be given in person with proof of identification or else the customer is directed to contact the owner of such data.

13.3 Members of staff dealing with customers on a daily basis should have suitable security questions which must always be used.

13.4 If a request for disclosure of information is received, you must:

- Obtain written consent from the customer that they are acting on their behalf.
- verify their identity, particularly if they request information via the telephone or in person.

13.5 In all circumstances, you must ensure you are legally able to share the information being requested and only share the minimum amount of information necessary.

14 Retention and Disposal of Information

14.1 Information must only be retained for as long as it is needed for business purposes, or in accordance with any statutory retention period

14.2 Staff should refer to the Council's Information Retention and Disposal Guidelines for further information. The Guidelines sets out the type of information held in service areas, together with statutory or agreed retention periods.

14.3 When disposing of information please ensure the most appropriate method is used. Paper files containing personal or sensitive information must be disposed of in the confidential waste bins. Electronic information must be permanently destroyed.

14.4 When shredding is involved, and a third-party is used, the Council must ensure that a certificate of destruction is produced and given. This would ideally include a general reference to the shredded contents and making a clear reference to the Disposal Log.

14.5 When purchasing new computer systems or software, please consider requirements for the

retention and disposal of information and ensure these are included at the scoping stage

14.6 All information destroyed in accordance with the Retention Schedule must be logged on the Disposal Log.

15 Vacating Premises or Disposing of Equipment

15.1 It is important that a process is in place to ensure all Council information is removed from premises should they be vacated and from equipment before it is disposed of. Equipment includes cupboards and filing cabinets as well as computers or other electronic devices.

15.2 The disposal of computer or other electronic devices is referenced in Section 25 of this policy and all electronic equipment must be returned to IT to be properly disposed of.

15.3 If the Council vacates any of its premises, the Executive Secretary must undertake appropriate checks of all areas, including locked rooms, basements and other storage areas, to ensure all Council information is removed. Such checks should be documented, dated and signed.

15.4 If information is bagged for disposal (whether confidential or not), this must be removed before the building is vacated.

15.5 Cupboards and filing cabinets must be checked before their disposal to ensure they contain no documents or papers. If a cupboard or cabinet is locked and no key is available, Campus should be asked to open it in order that it can be checked.

PART 2 – ICT SECURITY

16 Cloud Storage Solutions

16.1 The use of PERSONAL cloud storage solutions (such as Dropbox, Google Drive, Onedrive Personal, iCloud etc.) for the transfer of Council information is expressly forbidden. The Executive Secretary is to ensure that access is provided and recorded to Members of Staff who need to transfer Council information via its secure and official cloud storage solutions for the sharing of files.

16.2 Likewise, any system for data storage owed (in any manner) by the Council should be GDPR complaint and the Executive Secretary should ensure that certificates of compliance are produced at procurement stage.

17 Systems Development

17.1 All system developments must include security issues in their consideration of new developments, seeking guidance from professional sources, where appropriate and the Data Protection Officer for issues related to data protection.

17.2 Data Protection Impact Assessments (DPIAs) should be carried out prior to the purchase of any new system which will be used for storing and accessing personal information.

18 Network Security

18.1 The Council will engage a third-party specialist to routinely review network security.

19 Risks from Viruses

19.1 Viruses (including malware and zero-day threats) are one of the greatest threats to the Council's computer systems. PC viruses become easier to avoid with staff and members aware of the risks with unlicensed software or bringing data/software from outside the Council. Anti-virus measures reduce the risks of damage to the network.

19.2 Any suspected virus attacks must be reported to the Data Protection Officer and the third party specialist hired by the Council for its IT systems.

19.3 Members of Staff are to follow the Anti-virus guidelines that can be found at Appendix 1.

20 Cyber Security

20.1 Cyber security and cybercrime are increasing risks that, if left unchecked, could disrupt the day to day operations of the Council, the delivery of local public services.

20.2 The Council's approach to cyber security can be found in Appendix 2.

21 Access Control to Secure Areas

21.1 Secure areas include any areas where data is stored, being the Council's servers at the administrative offices, equipment for storing and viewing of CCTV footage and areas where photography is stored and any other location where personal data is kept, either in digital or printed format.

21.2 All Iż-Żejtun processors/networked file servers/Iż-Żejtun network equipment will be located in secure areas with restricted access.

21.3 Local network equipment/file servers and network equipment will be located in secure areas and where appropriate within locked cabinets.

21.4 Unrestricted access to the Iż-Żejtun computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment.

21.5 Restricted access may be given to other staff where there is a specific job function need for such access.

21.6 Authenticated representatives of third-party support agencies will only be given access through specific authorisation.

21.7 All secure areas will have an entry log which staff and visitors must use.

21.8 Regular reviews of who can access these secure areas should be undertaken.

22 Security of Third Party Access

22.1 No external agency will be given access to any of the Council's networks unless that body has been formally authorised by the Executive Secretary to have such access.

22.2 All external agencies will be required to sign security and confidentiality agreements with the Council.

22.3 All external agencies processing personal information on the Council's behalf (including via a hosted IT system) will be required to sign a third-party processing agreement.

22.4 The Council will control all external agencies access to its systems by enabling/disabling connections for each approved access requirement.

22.5 The Council will put in place adequate policies and procedures to ensure the protection of all information being sent to external systems. In doing so, it will make no assumptions as to the quality of security used by any third party but will request confirmation of levels of security maintained by those third parties. Where levels of security are found to be inadequate, alternative ways of sending data will be used.

22.6 All third parties and any outsourced operations will be liable to the same level of confidentiality as Council Staff.

23 Data Back-up

23.1 Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Information must not be held on a PC hard drive without the approval of the Executive Secretary.

23.2 Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes.

23.3 The backup copies should be clearly labelled and held in a secure area. Procedures should be in place to recover to a useable point after restart of this back-up. A cyclical system, whereby several generations of backup are kept, is recommended.

23.4 Archived and recovery data should be accorded the same security as live data and should be held separately preferably at an off-site location. Archived data is information, which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes. The Council's Retention Schedule must be followed in determining whether data should be archived.

23.5 Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested.

23.6 To ensure that, in an emergency, the back-up data is sufficient and accurate, it should be regularly tested. This can be done by automatically comparing it with the live data immediately after the back-up is taken and by using the back-up data in regular tests of the contingency plan.

23.7 Recovery data should be used only with the formal permission of the data owner or as defined in the documented contingency plan for the system.

23.8 If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data. This aims to ensure that back-up data is not corrupted in addition to the live data. A software or hardware engineer should check the relevant equipment or software using his/her own test data.

24 Equipment, Media and Data Disposal

24.1 If a machine has ever been used to process personal data as defined under the Data Protection Act or 'in confidence' data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken. Procedures for disposal should be documented on the Council's disposal log.

24.2 Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realise that data which may be sensitive is being stored automatically on their hard disk.

24.3 Although the software usually (but not always) deletes these files after they have served their purpose, they could be restored and retrieved easily from the disk by using commonly available utility software.

25 Software

25.1 All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action. Each user should ensure that a copy of each licence for commercial software is held.

25.2 The loading and use of unlicensed software on Council computing equipment is **NOT** allowed. All staff and members must comply with the Copyright Act (CAP 415). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. The Council monitors the installation and use of software by means of regular software audits; any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary by the Council.

25.3 The Council will only permit authorised software to be installed on its PCs. Approval will be via the Executive Secretary.

25.4 Where the Council recognises the need for specific specialised PC products, such products should be registered and be fully licensed.

25.5 Software packages must comply with and not compromise Council security standards.

25.6 Computers owned by the Council are only to be used for the work of the Council. The copying of leisure software on to computing equipment owned by the Council is not allowed.

25.7 Educational software for training and instruction should be authorised, properly purchased, virus checked and loaded by authorised representatives.

25.8 The Council seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas.

25.9 Users must be aware of the risk of viruses from email and the internet. If in doubt about any data received please contact the Data Protection Officer for anti-virus advice.

25.10 The Council shall endeavour to adopt an approach whereby it will conduct a market research

for business cloud solution prior to the purchase of any software.

26 Use of Removable Media

26.1 It is the Council's policy to prohibit the use of all unauthorised removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed.

26.2 All staff, Members and third parties must comply with the requirements regarding removable media.

27 Timeout Procedures

27.1 Inactive computers should be set to time out after a pre-set period of inactivity. The time-out facility should clear the screen. In high risk areas the time-out facility should also close both application and network sessions.

27.2 A high-risk area might be a public or external area outside the control of Council security management. The time-out delay should reflect the security risks of the area.

27.3 Users must 'lock' their computers, if leaving them unattended for any length of time. For high risk applications, connection time restriction should be considered. Limiting the period during which the computer has access to IT services reduces the window of opportunity for unauthorised access.

28 System Documentation

28.1 All systems should be adequately documented and should be kept up to date so that it matches the state of the system at all times.

28.2 System documentation, including manuals, should be physically secured (for example, under lock and key) when not in use.

28.3 Distribution of system documentation should be formally authorised by the Executive Secretary.

28.4 General Internet access carries with it a security risk of downloading viruses or programs that can look around a network and infiltrate password security systems. This information can then be sent back to the originator of the program in order to allow them unauthorised access to our systems. Therefore, care must be taken when transferring data.

29 Contact information regarding data protection

29.1 Members of the public and members of staff who wish to request more information about data protection in the Local Council should contact:

Data Protection Officer
c/o Iż-Żejtun Local Council
28, 'Dar iż-Żwieten', St. Angelo Street,
Iż-Żejtun ZTN 1369
Telephone: +356 7957 3417
Email: DPO@boomconsultancy.eu

Data Controller
The Executive Secretary
Iż-Żejtun Local Council
28, 'Dar iż-Żwieten', St. Angelo Street,
Iż-Żejtun ZTN 1369
Telephone: +356 2166 3866
Email: zejtun.lc@gov.mt

The Information and Data Protection Commissioner
Level 2, Airways House,
High Street,
Sliema, SLM 1549
Telephone: +356 2328 7100
Email: idpc.info@idpc.org.mt

30. APPROVALS AND SIGN OFFS

This policy comes into effect on 15 December 2019.

Document Control	
Approved By	**Executive Secretary**
Date approved	**10 December 2019**
Next review date	**09 December 2020**

This policy will be reviewed on an ongoing basis. The DPO is responsible for initiating each review.

31. VERSION CONTROL

Version	Date	Changes made by	Details
1.0	28/11/2019	DPO	Draft Information Security Policy

APPENDIX 1 - Anti-Virus Guidelines

1. What is a virus?

A computer virus is a damaging piece of software that can be transferred between programs or between computers without the knowledge of the user. When the virus software is activated (by incorporated instructions, e.g. on a particular date), it performs a range of actions such as displaying a message, corrupting software, files and data to make them unusable, and deleting files and/or data. While many of the viruses produced are benign and cause no real damage to the infected system, they always constitute a breach of security.

There is currently something like 60-75,000 known viruses and worms[1] - some 10-20 new viruses or variants appear a day. When a virus or worm is released into the public domain, network worms and mass mailer viruses can sometimes spread worldwide before anti-virus vendors have had time to produce updates.

Even daily anti-virus updates are not always enough to ensure safety from all possible threats.

2. What does the Council's IT Services do to prevent the spread of viruses?

Whilst precautions are taken at the network level to minimise the spread and impact of worms and viruses, it is not possible to make the process totally effective. Protection from viruses and worms is not a process that can be left entirely to system administrators, security officers, and anti-virus software. The best efforts of administrators and security experts are not sufficient - all computer users must also play their part by taking simple precautions like those described below.

3. Avoid Unauthorised Software

Programs like games, joke programs, cute screensavers, unauthorised utility programs and so on can sometimes be the source of difficulties even if they are genuinely non-malicious. That is why it is forbidden to install them. If such programs are claimed to be some form of antivirus or anti-Trojan[2] utility, there is a high risk that they are actually in some way malicious!

4. Treat all attachments with caution

It makes sense to be cautious about email attachments from people you don't know. However, if attachments are sent to you by someone you do know, don't assume they must be OK because you trust the sender.

---

[1] A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user.

[2] In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage. A Trojan horse may be widely redistributed as part of a computer virus.

Worms generally spread by sending themselves without the knowledge of the person from whose account they spread. If you do not know the sender or are not expecting any messages from the sender about that topic, it is worth checking with the sender that they intended to send a message, and if so, whether they intended to include any attachment. If you were expecting an attachment from them, this may not apply.

However, one recent virus sends out an email telling you that a ‘safe’ attachment is on the way, then sends out mail with a copy of itself as an attachment.

Bear in mind that even legitimate, expected attachments can be virus infected: worms and viruses are related, but cause slightly different problems.

Regard anything that meets the following criteria with particular suspicion:

- If they come from someone you don't know, who has no legitimate reason to send them to you.
- If an attachment arrives with an empty message.
- If there is some text in the message, but it doesn't mention the attachment.
- If there is a message, but it doesn't seem to make sense.
- If there is a message, but it seems uncharacteristic of the sender (either in its content or in the way it's expressed).
- If it concerns unusual material like pornographic web-sites, erotic pictures and so on.
- If the message doesn't include any personal references at all, (for instance a short message that just says something like "You must take a look at this", or "I'm sending you this because I need your advice” or “I love you!").
- If the attachment has a filename extension that indicates a program file (such as those listed below).
- If it has a filename with a ’double extension’, like FILENAME.JPG.vbs or FILENAME.TXT.scr, that may be extremely suspicious. As far as Windows is concerned, it's the last part of the name that counts, so check that against the list below to find out whether it's a program like those listed, masquerading as a data file, such as a text file or JPEG (graphics) file.

In all the above instances, it is recommended that you check with the sender that they knowingly sent the mail/attachment in question.

5. Avoid unnecessary macros

If Word or Excel warn you that a document you're in the process of opening contains macros[3], regard the document with particular suspicion unless you are expecting the document and you know that it's supposed to contain macros.

Even then, don't enable macros if you don't need to. It may be worth checking with the person who sent it to you that it is supposed to contain macros.

6. Be cautious with encrypted files

If you receive an encrypted (passworded) attachment, it will normally be legitimate mail from someone you know, sent intentionally (though the sender is unlikely to know in the event that they have a virus). However, that doesn't necessarily mean that it isn't virus-infected. If it started out infected, encryption won't fix it. Furthermore, encrypted attachments can't usually be scanned for viruses in transit: the onus is on the recipient to be sure the decrypted file is checked before it's opened. This goes not only for heavyweight encryption packages, but also for files compressed and encrypted with PKZip or WinZip.

7. Suspicious filename extensions

The following is a list of filename extensions that indicate an executable[4] program, or a data file that can contain executable programs in the form of macros. This list is by no means all-inclusive. There are probably a couple of hundred filename extensions that denote an executable program of some sort.

Furthermore, there are filenames like .RTF that shouldn't include program content, but sometimes can, while Word documents (for instance) can in principle have any filename extension, or none. Furthermore, zipped (compressed) files with the filename extension .ZIP can contain one or more of any kind of file.

.BAT	.CHM	.CMD	.COM	.DLL	.DOC	.DOT
.EXE	.FON	.HTA	.JS	.OVL	.PIF	.SCR
.SHB	.SHS	.VBS	.VBA	.WIZ	.XLA	.XLS

[3] In Microsoft Word and other programs, a macro is a saved sequence of commands or keyboard strokes that can be stored and then recalled with a single command or keyboard stroke. A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started.

[4] An executable is a file that contains a program. It is a particular kind of file that is capable of being executed or run as a program in the computer. In a Windows operating system, an executable file usually has a file name extension of .bat, .com, or .exe.

8. Report it!

If you think that you may have received a virus - report it!

APPENDIX 2 - Cyber Security Approach

1. Introduction

This document identifies the risks to the Council from main threats of cyber security and sets out what is in place to mitigate these risks.

If you do not understand anything in this document or feel you need specific training you should bring this to the attention of your line manager.

2. Purpose and Objectives

The document provides guidance to staff and members on the risks that threats from cyber security pose to the Council.

3. Roles and Responsibilities

The Council is responsible for the provision of the appropriate technology and technological devices to ensure that the Council is reasonably protected from the threats from cyber security.

The Executive Secretary is responsible ensuring that staff are communicated with about how to ensure that they don't put the Council at risk.

All employees, contractors and members should not take any action that puts the Councils systems or information at risk from cyber security. Any incidents must be reported in line with the Information Security policy.

4. Cyber Security

Cyber security and cybercrime are persistent threats that, if left unchecked, could disrupt the day to day operations of the Council, the delivery of local public services and ultimately have the potential to compromise national security. Additional costs will be incurred by the Council to rectify any cyber security or cybercrime event.

Technical advances create opportunities for greater efficiency and effectiveness. These include more engaging and efficient digital services, new ways to work remotely and to store and transfer data, such as mobile devices and cloud services.

The scale of targeted attacks, coupled with the difficulty of monitoring all possible attack methods requires the public sector to work together to both reduce the likelihood and the impact of such a threat succeeding.

Foreign states, criminals, hacktivists, insiders and terrorists all pose different kinds of threats. They may try to compromise public sector networks to meet various objectives.

5. Cyber Security Risks

The following types of cyber security all pose risks to the Council:

- Cybercrime:

  The most common form of cyber-attack against public bodies is the use of stolen or false customer credentials to commit fraud.

  The uptake in online services means this form of crime can now be undertaken on a much larger scale and can be international.

  Cybercriminals also seek to steal data from government networks that has a value on the black market, such as financial information or data that can be used for ID theft.

  There are several types of malware (malicious software) that have been written to specifically steal banking and log in information.

  The Council secures its network with up to date antivirus and malware protection, and manages the use of personal USB devices on Council computers.

- Hacktivism:

  Hacktivists seek to cause embarrassment or annoyance to the owners of high- profile websites and social media platforms that they may deface or take off line.

  When targeted against local government websites and networks, these attacks can cause reputational harm both locally and nationally.

  The Council has third party availability monitoring tools in place to alert key team members of the websites status.

- Insider threats:

  An insider is someone who exploits, or intends to exploit, their legitimate access to an organisation's assets for unauthorised purposes. Such activity can include:

  - Unauthorised disclosure of sensitive information
  - Facilitation of third party access to an organisation's assets
  - Physical sabotage
  - Electronic or IT sabotage

  Not all insiders deliberately set out to betray their organisation. An unwitting insider may compromise their organisation through poor judgment or due to a lack of understanding of security procedures.

  The insider threat is not new, but the environment in which insiders operate has changed significantly. Technology advances have created opportunities for staff at all levels to access information.

  The Council enforces the use of strong passwords for access to systems.

The Council only allows corporate USB devices to be written to. All personal USB devices are read only.

The Council uses mobile device management tools to secure corporate information on personal devices (smart phones and tablets).

The Council periodically reviews access to key IT systems.

6. The Council's approach to Cyber Security

The Council relies heavily on access to the internet and to information held in its systems. There are several IT systems that have an internet presence (website, webmail homeworking), and there are several different access mechanisms to information (Wi-Fi, physical networking, smartphones, tablets). All present threats to cyber security. It is widely acknowledged that it is not currently possible to keep out all attacks all of the time, but the Council employs a range of tools and good practice to minimise the risk to its information and systems.

The Council has clear polices on Information Security, which provide information on a range of areas including:

- Reporting of security incidents
- Use and security of emails
- Use of the internet
- Mobile phone usage
- Passwords
- Removable Media
- Clear desk policy
- Sharing and disclosing information
- Cloud storage systems
- Viruses
- Equipment, media and data disposal