# INFORMATION SECURITY
## POLICY

## 1. PURPOSE / DOEL

Computer information systems and networks are an integral part of business at The Eden District Municipality. The Eden District Municipality has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to:
1.1     Protect this investment.
1.2     Safeguard the information contained within these systems.
1.3     Reduce business and legal risk.
1.4     Protect the good name of the Eden District Municipality.

## 2. DEFENITIONS / DEFINISIE

Information is an asset, which like other important business assets, has value to an organization and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.  Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is characterized here as the preservation of:

2.1     Confidentiality: ensuring that information is accessible only to those authorized to have access
2.2     Integrity: safeguarding the accuracy and completeness of information and processing methods;
2.3     availability: ensuring that authorized users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met.

## 3. APPROVED / GOEDGEKEUR

EMC 32/05/07     **APPROVAL OF IT POLICIES, MAIL DISCLAIMER AND WEBSITE DISCLAIMER  / UPHUMEZO LWEMIGAQO YOBUCHWEPHESHA (079484)**

## 4. POLICY / BELEID

### 4.1 Violations:

Violations may result in disciplinary action in accordance with the Eden District Municipality policy. Failure to observe these guidelines may result in disciplinary action by the Eden District Municipality depending upon the type and severity of the violation, whether it causes any liability or loss to the Eden District Municipality, and/or the presence of any repeated violation(s).

### 4.2 Administration:

The information services manager (IS manager) is responsible for the administration of this policy.

### 4.3 Contents:

The topics covered in this document include:
4.3.1 Statement of responsibility
4.3.2 The Internet and e-mail
4.3.3 Computer viruses
4.3.4 Access codes and passwords
4.3.5 Physical security
4.3.6 Copyrights and license agreements

### *4.4 Statement of responsibility:*

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

#### *4.4.1 Manager responsibilities:*

Managers and supervisors must:
a) Ensure that all appropriate personnel are aware of and comply with this policy.
b) Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

#### *4.4.2 IS manager responsibilities:*

The IS manager must:
a) Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.

b) Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.

## 4.5   *The Internet and e-mail:*

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. One popular feature of the Internet is e-mail.

### 4.5.1  *Policy:*

Access to the Internet is provided to employees for the benefit of The Eden District Municipality and its customers. Employees are able to connect to a variety of business information resources around the world.

Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the Eden District Municipality's interests, the following guidelines have been established for using the Internet and e-mail.

### 4.5.2  *Acceptable use:*

Employees using the Internet are representing the Eden District Municipality. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner.

Examples of acceptable use are:
a) Using Web browsers to obtain business information from commercial Web sites.
b) Accessing databases for information as needed.
c) Using Email for business contacts.

### 4.5.3  *Unacceptable use:*

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the Eden District Municipality, or nonproductive.

Examples of unacceptable use are:
a) Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
b) Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list.
c) Conducting a personal business using the Eden District Municipality resources.
d) Transmitting any content that is offensive, harassing, or fraudulent.

### 4.5.4 *Downloads:*

File downloads from the Internet are <u>not</u> permitted unless specifically authorized in writing by the IS manager.

### 4.5.5 *Employee responsibilities:*

An employee who uses the Internet or Internet e-mail shall:
a) Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
b) Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached.
c) Not transmit copyrighted materials without permission.
d) Know and abide by all applicable policies dealing with security and confidentiality of the Eden District Municipality records.
e) Run a virus scan on any executable file(s) received through the Internet.
f) Avoid transmission of nonpublic customer information. If it is necessary to transmit nonpublic information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

### 4.5.6 *Copyrights:*

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the Eden District Municipality and/or legal action by the copyright owner.

### 4.5.7 *Monitoring:*

All messages created, sent, or retrieved over the Internet are the property of the Eden District Municipality and may be regarded as public information. The Eden District Municipality reserves the right to access the contents of any messages sent over its facilities if the Eden District Municipality believes, in its sole judgment, that it has a business need to do so. The Eden District Municipality therefore formally authorizes the IS Manager to access any messages if it is deemed necessary.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. **This means don't put anything into your e-mail**

**messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.**

### 4.6    Computer viruses:

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources.

#### 4.6.1  *Background:*

It is important to know that:
a)    Computer viruses are much easier to prevent than to cure.
b)    Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

#### 4.6.2  *IS responsibilities:*

IS shall:
a)    Install and maintain appropriate antivirus software on all computers.
b)    Respond to all virus attacks, destroy any virus detected, and document each incident.

#### 4.6.3  *Employee responsibilities:*

These directives apply to all employees:
a)    Employees shall not knowingly introduce a computer virus into the Eden District Municipality computers.
b)    Employees shall not load diskettes of unknown origin.
c)    Incoming diskettes shall be scanned for viruses before they are read.
d)    Any associate who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the IS manager.

### 4.7    Access codes and passwords:

The confidentiality and integrity of data stored on the Eden District Municipality computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

#### 4.7.1  *IS responsibilities:*

The IS manager shall be responsible for the administration of access controls to all the Eden District Municipality computer systems. The IS manager will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor.

Deletions may be processed by an oral request prior to reception of the written request The IS manager will maintain a list of administrative access codes and passwords and keep this list in a secure area.

### 4.7.2 *Employee responsibilities:*

Each employee:
a) Shall be responsible for all computer transactions that are made with his/her User ID and password.
b) Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.
c) Will change passwords at least every 90 days.
d) Should use passwords that will not be easily guessed by others.
e) Should log out when leaving a workstation for an extended period.

### 4.7.3 *Supervisor's responsibility:*

Managers and supervisors should notify the IS manager promptly whenever an employee leaves the Eden District Municipality or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

### 4.7.4 *Human resources responsibility:*

The Personnel Department will notify MIS monthly of associate transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

## 4.8 Physical security:

It is the Eden District Municipality policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

### 4.8.1 *Employee responsibilities:*

The directives below apply to all employees:
a)  Diskettes should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
b)  Diskettes should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
c)  Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.
d)  Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
e)  Since the IS manager is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IS.
f)  Employees shall not take shared portable equipment such as laptop computers out of the plant without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.
g)  Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

## 4.9 Copyrights and license agreements:

It is The Eden District Municipality's policy to comply with all laws regarding intellectual property.

### 4.9.1 *Legal reference:*

The Eden District Municipality and its employees are legally bound to comply with the Copyright Act 8 of 1978 and all proprietary software license agreements. Noncompliance can expose The Eden District Municipality and the responsible employee(s) to civil and/or criminal penalties.

### 4.9.2 *Scope:*

This directive applies to all software that is owned by The Eden District Municipality, licensed to The Eden District Municipality, or developed using The Eden District Municipality resources by employees or vendors.

### 4.9.3  *IS responsibilities:*

The IS manager will:
a)   Maintain records of software licenses owned by The Eden District Municipality.
b)   Periodically (at least annually) scan the Eden District Municipality computers to verify that only authorized software is installed.

### 4.9.4  *Employee responsibilities:*

Employees shall not:
a)   Install software unless authorized by IS. Only software that is licensed to or owned by The Eden District Municipality is to be installed on The Eden District Municipality computers.
b)   Copy software unless authorized by IS.
c)   Download software unless authorized by IS.

### 4.9.5  *Civil penalties:*

Violations of copyright law expose the Eden District Municipality and the responsible employee(s) to the following civil penalties:
a)   Liability for damages suffered by the copyright owner
b)   Profits that are attributable to the copying
c)   Fine for each illegal copy

### 4.9.6  *Criminal penalties:*

Violations of copyright law that are committed "willfully and for purposes of commercial advantage or private financial gain (copyright act 98 of 1978)," expose the Eden District Municipality and the employee(s) responsible to the following criminal penalties:
a)   Fines for each illegal copy
b)   Jail terms

## PASSWORD POLICY

1.   *Password Administration:*

Password administration is necessary to combat the forces that can compromise your valuable electronic resources. The two main forces are social engineering and brute force. Social engineering occurs when someone becomes familiar enough with a person to guess likely passwords. Brute force methods attack systems with systematically generated credentials attempting to guess a valid username and password. Both of these two enemies are capable of eventually

guessing a valid password and then exploiting resources and data on a corporate network.

Protecting your resources from these attacks is achievable through developing a solid password policy, diligence, and most importantly, using IT tools to enforce the policy.

2. Password Attributes:

| Character length | 05 characters or more |
|---|---|
| Expiration frequency | 30 Days |
| Password composition | None |
| Invalid login attempts | 5 unsuccessful attempts |
| Password history | A password must be unique from passwords used in the past. Users will be disallowed from reusing any of their previous 05 passwords. |
| Timeout = Logout | Have idle sessions disconnect from network resources after a specified period of inactivity. None. |
| Account Lock-out | 30 minutes after 5 unsuccessful |

This policy will be reviewed every 6 months.

## HELP DESK  POLICY

1.  Support:

Under normal operations, support will be given on a first-come, first-served basis and problems will be solved as soon as possible. However, the following ranking scheme should be used to categorize all requests for assistance. Additional consideration may be given to remote users. The contact and resolution times given below are the IT department's general guidelines under normal circumstances. During extraordinary situations, such as a natural disaster, prolonged power outage, or other catastrophic events, contact and resolution times may be longer.

| Priority | Issue | Contact | Resolution |
|---|---|---|---|
| 1 | Issue of the highest importance--mission-critical systems with a direct impact on the organization (Examples: widespread network outage, payroll system, sales system, telecom system, etc.) | Immediate-5 minutes | 30 minutes |

| | | | |
|---|---|---|---|
| 2 | Single user or group outage that is preventing the affected user(s) from working (Examples: failed hard drive, broken monitor, continuous OS lockups, etc.) | 15 minutes | 1 hour |
| 3 | Single user or group outage that can be permanently or temporarily solved with a workaround (Examples: malfunctioning printer, PDA synchronization problem, PC sound problem, etc.) | 30 minutes | Same Day |
| 4 | Scheduled work (Examples: new workstation installation, new equipment/software order, new hardware/software installation) | 1 hour | 1-4 days |
| 5 | Nonessential scheduled work (Examples: office moves, telephone moves, equipment loaners, scheduled events) | Same Day | 5 days |

## BACKUP POLICY

1.  Purpose:

    It is the policy of the IT Department (IT) to provide computer system backups to tape on a regular basis. The IT Department (IT)is responsible for implementing this policy. This document outlines what the policy means, and what benefits and costs accrue.

2.  Philosophy:

    The backup system is designed to recover from "catastrophic loss," meaning complete destruction of a machine, set of machines, or the entire site. It also covers disk hardware failure, where only part of a machine needs recovery. The purpose is disaster recovery as opposed to covering for user mistakes.

    A side effect of the backup system is the ability, in many cases, to restore individual files or sets of files for individual users. Doing this takes some time, thus priorities must be considered. Users are urged to ensure that their actions will bring about the desired results before pressing that last keystroke.

3.  Assumptions:

    It is assumed that:  The IT Department, and thus total disk storage, will continue to expand at a rate similar to what has been taking place over the past year; the

IT Department will remain heterogeneous in computing equipment types, and that the heterogeneity is likely to increase, with all platforms requiring support.

4.    Scheduling:

A complete current backup set will be moved offsite at least once per month. A complete current backup set will be made at least once per month for on—site storage. Incremental capability to restore those sets to more current status will be accomplished on approximately an everyworkday-evening basis.    Complete backup sets will be retained for a minimum of one year. Incremental sets will be maintained for a minimum of one month.  Backups will generally be performed at night and on weekends (local times). On occasion, particularly when a run fails, the IT Department (IT) will perform one or more backups during workdays, but th3se will be done with a goal of minimizing impact on users while accomplishing the backup, and only when necessary.

This schedule means that not all files will be recoverable at any given time. Machines can be restored to the status they were in on a given day at the time the backup was initiated. Any files created (or versions of files modified) after one backup ran then modified or deleted prior to the next run will not be restorable. Files not present at the time of a monthly backup will not be recoverable after the incremental tapes are recycled (generally a few months later).

5.    Restorations:

Machines requiring recovery from disk damage or other catastrophic loss will be restored as best possible at high priority. User file restorations will be handled as time permits.

6.    Verification:

Once per week the backup system will be tested by restoring a single random file from a random machine, and manually inspecting it for accurate restoral. Once per month a similar test will be made using an entire directory. These restoral tests will be performed into temporary areas so that current "real" user copies of the files will not be overwritten.The form of manual inspection will vary with the type of file(s) restored. Text may be "diff"ed or inspected manually. Binaries may be binary "diff"ed where the tape copy is still current, may be run in some cases, or may be dumped in hexadecimal format for manual comparison.

## ELECTRONIC MAIL AND INTERNET CONTENT POLICY

1.    Introduction:

This document specifies what content will be allowed to be send and received via Email and content to be viewed via the internet.

2.    Email Content:

2.1    Attachments:

Currently all attachment, except executable files are permitted to be transferred. This policy is subject to change pending future monitoring.

2.2    Size:

Currently all users are restricted to 2.5MB of content being received and sent. This policy is subject to change pending future monitoring.

2.3    Spam and Other:

No spamming is allowed and software is in place to monitor and prohibit this action.

**3**.    Current Policies:

| POLICY NAME | ENABLE POLICY | MESSAGE TYPE | SYNONYMS CHECKING | ACTION | EDIT POLICY | OPTIONS | DELETE POLICY |
|---|---|---|---|---|---|---|---|
| Anti-Spam | Enable | In & Outbound | Off | Quarantine | | Options | |
| Dirty WordS | Enable | In & Outbound | Off | Delete | Edit | Options | Delete |
| Ratial Discrimination | Enable | In & Outbound | Off | Delete | Edit | Options | Delete |
| Sexual Discrimination | Enable | In & Outbound | Off | Delete | Edit | Options | Delete |
| E-Greeting Card | Enable | In & Outbound | Off | Delete | Edit | Options | Delete |
| Melissa Virus | Enable | In & Outbound | Off | Delete | Edit | Options | Delete |
| Block HTML script messages | Enable | In & Outbound | Off | Delete | Edit | Options | Delete |

4.    Internet Content:

Internet content is filtered, restricted, monitored and reported on the following criteria.

| WORK TIME | LEISURE TIME |
|---|---|
| ✓ Violence / Profanity | ✓ Violence / Profanity |
| ✓ Partial Nudity | ✓ Partial Nudity |
| ✓ Full Nudity | ✓ Full Nudity |
| ✓ Sexual Acts | ✓ Sexual Acts |
| ✓ Gross Depictions | ✓ Gross Depictions |
| ✓ Intolerance | ✓ Intolerance |
| ✓ Satanic or Cult | ✓ Satanic or Cult |
| ✓ Drugs / Drug Culture | ✓ Drugs / Drug Culture |
| ✓ Militant / Extremist | ✓ Militant / Extremist |
| Sex Education | Sex Education |
| ✓ Questionable / Illegal & Gambling | ✓ Questionable / Illegal & Gambling |
| ✓ Alcohol & Tobacco | ✓ Alcohol & Tobacco |
| Sports & Entertainment | Sports & Entertainment |
| Search Engines | Search Engines |

This policy is subject to change pending future monitoring. This policy shall be reviewed every 6 months.

## 5. PROCESS / PROSES

## 6. APPLICABLE FORMS / TOEPASLIKE VORMS

Annexure A

# ACKNOWLEDGMENT OF INFORMATION SECURITY POLICY

This form is used to acknowledge receipt of, and compliance with, the Eden District Municipality Information Security Policy.

## 1. *Procedure:*

Complete the following steps:

1.1 Read the Information Security Policy.
1.2 Sign and date in the spaces provided below.
1.3 Return this page only to the information services manager.

## 2. Signature:

By signing below, I agree to the following terms:

2.1 I have received and read a copy of the "Information Security Policy" and understand the same;
2.2 I understand and agree that any computers, software, and storage media provided to me by the Eden District Municipality contains proprietary and confidential information about The Eden District Municipality and its customers or its vendors, and that this is and remains the property of the Eden District Municipality at all times;
2.3 I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at The Eden District Municipality), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;
2.4 I agree that, if I leave The Eden District Municipality for any reason, I shall immediately return to the Eden District Municipality the original and copies of any and all software, computer materials, or computer equipment that I may have received from the Eden District Municipality that is either in my possession or otherwise directly or indirectly under my control.

Employee signature: _____

Employee name: _____

Date: _____

Department: _____