CAPE WINELANDS DISTRICT
MUNICIPALITY • MUNISIPALITEIT • UMASIPALA

# INFORMATION TECHNOLOGY SECURITY POLICY

**POLICY ADOPTED BY COUNCIL ON 24 MAY 2005**
**AT ITEM MC 7.3**

# Cape Winelands District Municipality Information Technology Security Policy

## TABLE OF CONTENTS

## 1. Preamble

1.1 The Cape Winelands District Municipality (CWDM) acknowledges an obligation to ensure appropriate security for all Information Technology data, equipment, and processes in its domain of ownership and control. This obligation is shared, to varying degrees, by every member of the CWDM.

1.2 This document will:

1.2.2 Enumerate the elements that constitute IT security.
1.2.3 Explain the need for IT security.
1.2.4 Specify the various categories of IT data, equipment, and processes subject to this policy.
1.2.5 Indicate, in broad terms, the IT security responsibilities of the various roles in which each member of the CWDM may function.
1.2.6 Indicate appropriate levels of security through standards and guidelines.

## 2. Scope of IT Security

2.1 Definition of Security

2.1.1 Security can be defined as "the state of being free from unacceptable risk". The risk concerns the following categories of losses:

2.1.1.1 Confidentiality of Information.

2.1.1.1.1 Confidentiality refers to the privacy of personal or corporate information. This includes issues of copyright.

2.1.1.2 Integrity of data.

2.1.1.2.1 Integrity refers to the accuracy of data. Loss of data integrity may be gross and evident, as when a computer disc fails, or subtle, as when a character in a file is altered.

2.1.1.3 Assets.

2.1.1.3.1 The assets that must be protected include:

2.1.1.3.1.1 Computer and Peripheral Equipment.
2.1.1.3.1.2 Communications Equipment.
2.1.1.3.1.3 Computing and Communications Premises.

2.1.1.3.1.4 Power, Water, Environmental Control, and Communications utilities.
2.1.1.3.1.5 Supplies and Data Storage Media.
2.1.1.3.1.6 System Computer Programs and Documentation.
2.1.1.3.1.7 Application Computer Programs and Documentation.
2.1.1.3.1.8 Information.

2.1.1.4 Efficient and Appropriate Use.

2.1.1.4.1 Efficient and Appropriate Use ensures that CWDM IT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others.

2.1.1.5 System Availability.

2.1.1.5.1 Availability is concerned with the full functionality of a system (e.g. finance or payroll) and its components. The potential causes of these losses are termed "threats". These threats may be human or non-human, natural, accidental, or deliberate.

2.2 Domains of Security

2.2.1 This policy will deal with the following domains of security:

2.2.1.1 Computer system security: CPU, Peripherals, OS. This includes data security.

2.2.1.2 Physical security: The premises occupied by the IT personnel and equipment.

2.2.1.3 Operational security: Environment control, power equipment, operation activities.

2.2.1.4 Procedural security by IT, vendor, management personnel, as well as ordinary users.

2.2.1.5 Communications security: Communications equipment, personnel, transmission paths, and adjacent areas.

## 3 Reasons for IT Security

3.1 Confidentiality of information is mandated by common law, formal statute, explicit agreement, or convention. Different classes of information warrant different degrees of confidentiality.

3.2 The hardware and software components that constitute the CWDM's IT assets represent a sizable monetary investment that must be protected. The same is true for the information stored in its IT systems, some of which may have taken huge resources to generate, and some of which can never be reproduced.

3.3 The use of CWDM IT assets in a manner other than the purpose for which they were originally intended represents a misallocation of valuable CWDM resources, and possibly a danger to its reputation or a violation of the law.

3.4 Finally, proper functionality of IT systems is required for the efficient operation of the CWDM. Some systems, such as the VIP Payroll and SAMRAS systems are of paramount importance to the mission of the CWDM.

## 4 Roles and Responsibilities

### 4.1 Policy Management

4.1.1 Approval of the IT Security Policy is vested with the Council of the CWDM.

4.1.2 Advice and opinions on the Policy will be given by:

4.1.3 Information Technology Steering Committee (ITSC)

4.1.4 Formulation and maintenance of the policy is the responsibility of the IT department.

### 4.2 Policy Implementation

4.2.1 Each member of the CWDM will be responsible for meeting published IT standards of behavior.

4.2.2 IT security of each system will be the responsibility of its custodian.

4.3 Custodians

4.3.1 The IT Department will be the custodian of all strategic system platforms.
4.3.2 The IT Department will be custodian of the strategic communications systems.
4.3.3 The IT Department will be custodian of strategic applications whilst the management control (e.g. Finance, HR, etc) will reside with the applicable executive directorate.
4.3.4 The IT Department will be custodian of desktop systems whilst the management control will reside with the individual responsible for the desktop.

4.4 Individuals

4.4.1 All ordinary users of CWDM IT resources:

4.4.1.1 Will operate under the "Conditions of Use" provisions of the "Standards and Guidelines for All Users of CWDM Computing and Network Facilities."
4.4.1.2 Must behave under the "Code of Practice" provisions of the "Standards and Guidelines for All Users of CWDM Computing and Network Facilities."
4.4.1.3 Are responsible for the proper care and use of IT resources under their direct control.

4.5 CWDM Services

4.5.1 It is recognized that various sections of the CWDM provide services that relate to IT security, both directly and indirectly. It is expected that there will be collaboration between these sections and the IT department in generation of standards and implementation of the policy. Some of these sections and their services are:

4.5.1.1 Human Resources: Personnel selection, induction, and exit-processing.
4.5.1.2 Registrar: Policies concerning confidentiality privacy, and copyright.
4.5.1.3 CWDM Services: Physical building security.

### 4.6 Standards and Guidelines

4.6.1 Standards (mandatory) and guidelines (suggestions) will be published as attachments to this policy to assist ordinary users and system custodians to meet their IT security responsibilities. These standards and guidelines are an integral part of the CWDM IT Security Policy and therefore define it in detail.

4.6.2 These Standards and Guidelines will appear under the following classifications:

4.6.2.1 Personal behaviour.
4.6.2.2 Strategic systems.
4.6.2.3 Computer.
4.6.2.4 Communications.
4.6.2.5 Desktop (personal) systems.

## 5 Policy Documentation

### 5.1 Documents

5.1.1 This policy is enunciated by 3 documents:

5.1.1.1 "Standards and Guidelines for All Users of CWDM Computing and Network Facilities".

5.1.1.2 "Standards and Guidelines for Strategic Systems".

5.1.1.3 "Standards and Guidelines for Desktop Computers."

### 5.2 Availability

5.2.1 It is intended that this IT Security Policy be publicly accessible in its entirety. There is the requirement that all users of CWDM IT resources be familiar with relevant sections of this policy.

### 5.3 Changes

5.3.1 The IT Security Policy is a "living" document that will be altered as required to deal with changes in technology, applications, procedures, legal and social imperatives, perceived dangers, etc.

5.3.2 Major changes will be made in consultation with the IT Steering Committee and with the approval of Council.

5.3.3 Minor changes will be approved by the Municipal Manager of the CWDM and brought to the attention of IT Steering Committee and Council.

# 6 Standards and Guidelines for all users of CWDM Computing and Network Facilities

## 6.1 Conditions of Use of Computing and Networking Facilities

6.1.1 It is the policy of the CWDM that it's computing and networking facilities are intended for work-related use in support of the CWDM's mission. Although recognizing the increasing importance of these facilities to the activities of staff, the CWDM reserves the right to limit, restrict, or extend access to them.

6.1.2 All persons using the computing and networking facilities shall be responsible for the appropriate use of the facilities provided as specified by the "Codes of Practice" of this policy, and shall observe conditions and times of usage as published by the Administrator of the system.

6.1.3 It is the policy of the CWDM that it's computing and associated network facilities are not to be used for commercial purposes or non-work-related activities without written authorization from the CWDM. In any dispute as to whether work carried out on the computing and networking facilities is internal work, the decision of the Municipal Manager shall be final.

6.1.4 The user will not record or process information which knowingly infringes any patent or breaches any copyright.

6.1.5 The CWDM will endeavour to protect the confidentiality of information and material furnished by the user and will instruct all computing personnel to protect the confidentiality of such information and material. The CWDM shall be under no liability in the event of any improper disclosure.

6.1.6 The CWDM will endeavour to safeguard the possibility of loss of information within the CWDM's computing and networking facilities but will not be liable to the user in the event of any such loss. The user must take all reasonable measures to further safeguard against any loss of information within the CWDM's computing and networking facilities.

6.1.7 If a loss of information within the system can be shown to be due to negligence on the part of the computing or network personnel employed by the CWDM, or to any hardware or software failure which is beyond the user's means to avoid or control, then the IT Department will endeavour to help restore the information.

6.1.8 The use of the computing and networking facilities is permitted by the CWDM on the condition that it will not involve the infringement of any patent or the breach of any copyright and the user agrees to indemnify and

keep indemnified the CWDM and each member and every member of its staff against all actions, claims, and demands for infringement of patent and or breach of copyright which may be brought or made against the CWDM or any member of its staff arising out of or in connection with the use of the computing and networking facilities.

6.1.9 Users and Department Heads are expected to complete an IT Support Form for any IT-related queries. This Support Form must be handed in to the IT Department before the respective queries can be actioned. Failure to comply with the aforementioned will result in no assistance from the IT Department.

6.1.10 It is the policy of the CWDM to replace Desktop PCs and Notebooks every three years. However, approval for the purchase or replacement of Notebooks must be motivated by the head of department. All requests for the purchase of software, hardware and IT-related products and services have to be approved by IT, to ensure that proper standards are adhered to. This is to ensure that items purchased fall in line with the technology and maintenance roadmap of the CWDM.

6.1.11 Users are prohibited from connecting any hardware (especially personal hardware) with network functionality to the CWDM network without prior approval.

6.1.12 Users of the computing and networking facilities recognize that when they cease to be formally associated with the CWDM (e.g. no longer an employee to the CWDM), their access will be removed from CWDM computing and networking facilities without notice.

6.1.13 The CWDM reserves the right to limit permanently or restrict any user's usage of the computing and networking facilities; to copy, remove, or otherwise alter any information or system that may undermine the authorized use of the computing and networking facilities; and to do so with or without notice to the user in order to protect the integrity of the computing and networking facilities against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage.

6.1.14 The CWDM, through authorized individuals, reserves the right to periodically check and monitor the computing and networking facilities, and reserves any other rights necessary to protect the computing and networking facilities.

6.1.15 The CWDM disclaims responsibility and will not be responsible for loss or disclosure of user information or interference with user information resulting from its efforts to maintain the privacy, security and integrity of the computing and networking facilities and information.

6.1.16 The CWDM reserves the right to take emergency action to safeguard the integrity and security of the computing and networking facilities. This includes but is not limited to the termination of a program, job, or on-line session, or the temporary alteration of user account names and passwords. The taking of emergency action does not waive the rights of the CWDM to take additional actions under this policy.

6.1.17 Users of the computing and networking facilities do so subject to applicable legislation and CWDM policies. The CWDM disclaims any responsibility and/or warranties for information and materials residing on non-CWDM computer systems or available over publicly accessible networks, except where such responsibility is formally expressed. Such materials do not necessarily reflect the attitudes, opinions, or values of the CWDM, or its staff.

6.1.18 The Manager of the IT Department may suspend any person from using the computing and networking facilities for a period not exceeding 28 days (and may recommend additional penalties to the Municipal Manager) if after appropriate investigation that person is found to be:-

6.1.18.1.1 responsible for willful physical damage to any of the computing and networking facilities;
6.1.18.1.2 in possession of confidential information obtained improperly;
6.1.18.1.3 responsible for willful destruction of information;
6.1.18.1.4 responsible for deliberate interruption of normal services provided by the IT Department;
6.1.18.1.5 responsible for the infringement of any patent or the breach of any copyright;
6.1.18.1.6 gaining or attempting to gain unauthorized access to accounts and passwords;
6.1.18.1.7 gaining or attempting to gain access to restricted areas without the permission of the IT Manager;
6.1.18.1.8 responsible for inappropriate use of the facilities.

6.1.19 External work or use of the computing and networking facilities shall not be undertaken which would prevent CWDM users from having their usual access to the facilities.

6.1.10 External users of the CWDM's computing and networking facilities must adhere to the CWDM's policy on access to the Internet which prohibits direct connectivity to the Internet to individuals and organizations outside of the CWDM.

## 6.2 Code of Practice in the Use of Computing & Network Facilities

### 6.2.10 INTRODUCTION

6.2.10.1 Standards for the use of the CWDM's computing and networking facilities derive directly from standards of common sense and common decency that apply to the use of any shared resource. The CWDM community depends on a spirit of mutual respect and cooperation to resolve differences and resolve problems that arise from time to time. This code of practice is published in that spirit. Its purpose is to specify user responsibilities and to promote the appropriate use of IT for the protection of all members of the CWDM community.

### 6.2.11 APPROPRIATE AND REASONABLE USE

6.2.11.1 Appropriate and responsible use of the CWDM computing and networking facilities is defined as use that is consistent with the teaching, learning, research and administrative objectives of the CWDM and with the specific objectives of the project or task for which such use was authorized. All uses inconsistent with these objectives are considered to be inappropriate use.

### 6.2.12 RESPONSIBILITIES

6.2.12.1 Users of the CWDM computing and networking facilities accept the following specific responsibilities:

6.2.12.1.1 Security:

6.2.12.1.1.1 To safeguard their data, personal information, passwords and authorization codes, and confidential information;
6.2.12.1.1.2 To take full advantage of file security mechanisms built into the computing systems;
6.2.12.1.1.3 To choose their passwords wisely and to change them periodically;
6.2.12.1.1.4 To follow the security policies and procedures established to control access to and use of administrative data.

6.2.12.1.2 Confidentiality:

6.2.12.1.2.1 To respect the privacy of other users; for example, not to intentionally seek information on, obtain copies of, or modify files, tapes, or passwords belonging to other users or the CWDM;
6.2.12.1.2.2 Not to represent others, unless authorized to do so explicitly by those users;

6.2.12.1.2.3 Not to divulge sensitive personal data to which they have access concerning staff without explicit authorization to do so.

6.2.12.1.2.4 To respect the rights of other users; for example, to comply with all CWDM policies regarding sexual, racial, and other forms of harassment. The CWDM is committed to being a racially, ethnically, and religiously heterogeneous community.

6.2.12.1.2.5 To respect the legal protection provided by copyright and licensing of programs and data; for example, not to make copies of a licensed computer program to avoid paying additional license fees or to share with other users.

6.2.12.1.2.6 To respect the intended usage of resources; for example, to use only the account name and password, funds, transactions, data, and processes assigned by service providers, unit heads, or project directors for the purposes specified, and not to access or use other account names and passwords, funds, transactions, data, or processes unless explicitly authorized to do so by the appropriate authority.

6.2.12.1.2.7 To respect the intended usage of systems for electronic exchange (such as e-mail, internet, etc.); for example, not to send forged electronic mail, mail that will intimidate or harass other users, chain messages that can interfere with the efficiency of the system, or promotional mail for profit-making purposes. Also, not to break into another user's electronic mailbox or read someone else's electronic mail without their permission.

6.2.12.1.2.8 To respect the integrity of the computing and networking facilities; for example, not to intentionally develop or use programs, transactions, data, or processes that harass other users or infiltrate the system or damage or alter the software or data components of a system. Alterations to any system or network software or data component are to be made only under specific instructions from authorized staff, unit heads, project directors, or management staff.

6.2.12.1.2.9 To respect the financial structure of the computing and networking facilities; for example, not to intentionally develop or use any unauthorized mechanisms to alter or avoid charges levied by the CWDM for computing, network, and data processing services.

6.2.12.1.2.10 To adhere to all general CWDM policies and procedures including, but not limited to, policies on proper use of information resources, computing and networking facilities; the acquisition, use,

and disposal of CWDM-owned computer equipment; use of telecommunications equipment; legal use of software; and legal use of administrative data.

6.2.12.1.2.11 To report any information concerning instances in which the CWDM IT Security Policy or any of its standards and codes of practice has been or is being violated. In general, reports about violations should be directed to the Head of the IT Department.

6.2.13 CODE OF PRACTICE FOR SPECIFIC ACTIVITIES

6.2.13.1 The following apply to specific activities.

6.2.13.1.1 Illegal activity

6.2.13.1.1.1 In general, it is inappropriate use to store and/or give access to information on the CWDM computing and networking facilities that could result in legal action against the CWDM.

6.2.13.1.2 Objectionable material

6.2.13.1.2.1 The CWDM's computing and networking facilities must not be used for the transmission, possession, demonstration or advertisement of objectionable or illegal material.

6.2.13.1.3 Restricted Software and Hardware

6.2.13.1.3.1 Users should not knowingly possess, give to another person, install on any of the computing and networking facilities, or run, programs or other information which could result in the violation of any CWDM policy or the violation of any applicable license or contract. This is directed towards but not limited to software known as viruses, Trojan horses, worms, password breakers, and packet observers. Authorization to possess and use Trojan horses, worms, viruses and password breakers for legitimate research or diagnostic purposes can be obtained from the IT Manager.

6.2.13.1.3.2 The unauthorized physical connection of monitoring devices to the computing and networking facilities which could result in the violation of CWDM policy or applicable licenses or contracts is inappropriate use. This includes but is not limited to the attachment of any electronic device to the computing and networking facilities for the purpose of monitoring data, packets, signals or other information. Authorization to possess and use such hardware for legitimate diagnostic purposes must be obtained from the IT Manager of the IT Department.

6.2.13.1.4 Copying and Copyrights

6.2.13.1.4.1 Users of the computing and networking facilities must abide by the CWDM Copyright Policy, which covers copyright issues pertaining to CWDM staff as well as commissioned works of non-employees.

6.2.13.1.4.2 Respect for intellectual labour and creativity is essential to academic discourse. This tenet applies to works of all authors and publishers in all media. It includes respect for the right to acknowledgment and right to determine the form, manner, and terms of publication and distribution. If copyright exists, as in most situations, it includes the right to determine whether the work may be reproduced at all. Because electronic information is volatile and easily reproduced or altered, respect for the work and personal expression of others is especially critical in computing and networking environments. Viewing, listening to or using another person's information without authorization is inappropriate use of the facilities. Standards of practice apply even when this information is left unprotected.

6.2.13.1.4.3 In particular, users should be aware of and abide by the CWDM Policy on Copying and Using Computer Software. Most software that resides on the computing and networking facilities is owned by the CWDM or third parties, and is protected by copyright and other laws, together with licenses and other contractual agreements. Users are required to respect and abide by the terms and conditions of software use and redistribution licenses. Such restrictions may include prohibitions against copying programs or data for use on the computing and networking facilities or for distribution outside the CWDM; against the resale of data or programs, or the use of them for non-educational purposes or for financial gain; and against public disclosure of information about programs (e.g., source code) without the owner's authorization. CWDM employees who develop new packages that include components subject to use, copying, or redistribution restrictions have the responsibility to make any such restrictions known to the users of those packages.

6.2.13.1.5 Harassment

6.2.13.1.5.1 CWDM policy prohibits sexual and discriminatory harassment. CWDM's computing and networking facilities are not to be used to libel, slander, or harass any other person. The following constitute examples of Computer Harassment:

6.2.13.1.5.1.1 Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or

threats of bodily harm to the recipient or the recipient's immediate family;

6.2.13.1.5.1.2 Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;

6.2.13.1.5.1.3 Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease;

6.2.13.1.5.1.4 Intentionally using the computer to disrupt or damage the research, administrative, or work-related pursuits of another;

6.2.13.1.5.1.5 Intentionally using the computer to invade the privacy, work-related or otherwise, of another or the threatened invasion of the privacy of another.

6.2.13.1.5.1.6 The display of offensive material in any publicly accessible area is likely to violate CWDM harassment policy. There are materials available on the Internet and elsewhere that some members of the CWDM community will find offensive. The CWDM cannot restrict the availability of such material, but it considers its display in a publicly accessible area to be inappropriate. Public display includes, but is not limited to, publicly accessible computer screens and printers.

6.2.13.1.6 Wasting Resources

6.2.13.1.6.1 It is inappropriate use to deliberately perform any act which will impair the operation of any part of the computing and networking facilities or deny access by legitimate users to any part of them. This includes but is not limited to wasting resources, tampering with components or reducing the operational readiness of the facilities.

6.2.13.1.6.2 The willful wasting of computing and networking facilities resources is inappropriate use. Wastefulness includes but is not limited to passing chain letters, random mailing, willful generation of large volumes of unnecessary printed output or disk space, willful creation of unnecessary multiple jobs or processes, or willful creation of heavy network traffic. In particular, the practice of willfully using the CWDM's computing and networking facilities for the establishment of

frivolous and unnecessary chains of communication connections is an inappropriate waste of resources.

6.2.13.1.6.3 The sending of random mailings ("chain mail") is not permitted as such activities are in direct violation of existing policy. It is also poor etiquette at best, and harassment at worst, to deliberately send unwanted mail messages to strangers. Recipients who receive junk mail should request the assistance of the IT department, so that appropriate measures can be taken to ensure that such mail is blocked.

6.2.13.1.7 Commercial Use

6.2.13.1.7.1 CWDM computing and network facilities are provided by CWDM for the support of its mission. It is inappropriate to use the computing and networking facilities for:

6.2.13.1.7.1.1 Commercial gain or placing a third party in a position of commercial advantage

6.2.13.1.7.1.2 Any non-CWDM related activity, including non-CWDM related communications

6.2.13.1.7.1.3 Commercial advertising or sponsorship except where such advertising or sponsorship is clearly related to or supports the mission of the CWDM or the service being provided.

6.2.13.1.7.1.4 This paragraph is not intended to restrict free speech or to restrict the CWDM from setting up Information servers or other services specifically designated for the purpose of fostering an "electronic community" with the wider community the CWDM serves. These designated Information servers should normally conform to the CWDM IT Security Policy of which this Code of Practice is a part.

6.2.13.1.8 Usage

6.2.13.1.8.1 CWDM computing and network facilities may not be used in connection with compensated and/or non-compensated outside work nor for the benefit of organizations not related to CWDM.

6.2.13.1.9 Additional Guidelines at Local Sites

6.2.13.1.9.1 The CWDM computing and network facilities are composed of many "sites." Each site may have local rules and regulations which govern the use of computing and network facilities at that site. Each site has operators, consultants, and/or supervisors who have been

given the responsibility to supervise the use of that site. Users are expected to cooperate with these individuals and comply with CWDM and local site policies. Site policies may be more restrictive than CWDM policy. It is the intention that the CWDM IT Security Policy represent a minimum standard.

6.2.13.1.10 Use of Desktop Systems and Notebooks

6.2.13.1.10.1 Users are responsible for the security and integrity of CWDM information stored on their personal desktop system and/or notebook. This responsibility includes making regular disk backups on to the user's designated area on the CWDM network, controlling physical and network access to the machine. Users should avoid storing passwords or other information that can be used to gain access to CWDM resources. Users should not store CWDM passwords or any other confidential data or information on their notebook, home PC, associated flash disks or CD's. All such information should be secured and backed up on to the user's designated area on the CWDM network. These designated areas are included in the CWDM Backup Policy.

6.2.13.1.11 Printouts

6.2.13.1.11.1 Users are responsible for the security and privacy of printouts of CWDM information.

6.2.13.1.12 Software Security

6.2.13.1.12.1 CWDM computer software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-CWDM party for any purposes other than CWDM purposes expressly authorized by the IT Department or Department Heads.

6.2.13.1.12.2 Exchanges of software and/or data between CWDM and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

6.2.13.1.12.3 The CWDM strongly supports strict adherence to software vendors' license agreements. Adherence to these agreements is subject to random audits by these vendors. When CWDM computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.

6.2.13.1.13 Reporting Security Problems

6.2.13.1.13.1 The IT Department must be notified immediately when:

6.2.13.1.13.1.1 Sensitive CWDM information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties.

6.2.13.1.13.1.2 Unauthorized use of CWDM information systems has taken place, or is suspected of taking place.

6.2.13.1.13.1.3 Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed.

6.2.13.1.13.1.4 There is any unusual systems behavior, such as missing files, frequent system crashes, misrouted messages.

6.2.13.1.13.1.5 Security problems should not be discussed widely but should instead be shared on a need-to-know basis.

6.2.13.1.13.1.6 Users must not attempt to probe computer security mechanisms at the CWDM or other Internet sites.

6.2.13.1.13.1.7 Unless prior written authority has been obtained from the Manager of the IT Department, files containing hacking tools or other suspicious material may be taken as prima facie evidence of unauthorized hacking activity and may expose the user to disciplinary procedures.

6.2.13.1.14 User Indemnity

6.2.13.1.14.1 Users agree to indemnify the CWDM for any loss or damage arising out of improper use.

6.2.13.1.15 Limited Warranty

6.2.13.1.15.1 The CWDM takes no responsibility and provides no warranty against the non-delivery or loss of any files, messages or data nor does it accept any liability for consequential loss in the event of improper use or any other circumstances.

6.2.13.1.16 Penalties

6.2.13.1.16.1 Violations of these computer security policies can lead to withdrawal and/or suspension of system and network privileges and/or disciplinary action.

## 6.3 Appropriate Use of Electronic Mail

6.3.10 Preamble

6.3.10.1 Electronic mail and communications facilities provided by the CWDM are intended for work-related and administrative purposes. Their use is governed by CWDM rules and policies, applicable legislation, and acceptable use policy of the provider.

6.3.10.2 Electronic mail may be used for personal communications within appropriate limits.

6.3.11 Scope

6.3.11.1 These Standards of Use cover all electronic mail systems used by members of the CWDM community, from the CWDM's network or connecting to the CWDM's network or while acting in an official CWDM capacity.

6.3.12 Appropriate Use and Responsibility of Users

6.3.12.1 Electronic mail can be both informal like a phone call and yet irrevocable like an official memorandum. Because of this, users should explicitly recognize their responsibility for the content, dissemination and management of the messages they send. This responsibility means ensuring that messages:

6.3.12.1.1 Do not contain information that is harmful to the CWDM or members of the CWDM community;
6.3.12.1.2 Are courteous and polite;
6.3.12.1.3 Are consistent with CWDM policies;
6.3.12.1.4 Protect others' right to privacy and confidentiality;
6.3.12.1.5 Do not contain obscene, offensive or slanderous material;
6.3.12.1.6 Are not used for purposes that conflict with the CWDM's interests;
6.3.12.1.7 Contain an accurate, appropriate and informative signature;
6.3.12.1.8 Do not unnecessarily or frivolously overload the email system (e.g. chain mails, spamming and junk mail is not allowed);
6.3.12.1.9 Are not for commercial purposes unless authorized by the CWDM.

6.3.12.2 Users should cover periods of absence by adopting an appropriate functional account, forward, or vacation message strategy.

6.3.12.3 Electronic mail containing a formal approval, authorization, delegation or handing over of responsibility must be copied to paper and filed appropriately for purposes of evidence and accountability.

6.3.13 Confidentiality and Security

6.3.13.1 Electronic mail is inherently NOT SECURE.

6.3.13.2 As CWDM networks and computers are the property of the CWDM, the CWDM retains the right to allow the IT department to monitor internet usage.

6.3.13.3 It is recommended that personal confidential material not be stored on or sent through CWDM equipment.
6.3.13.4 Users must ensure the integrity of their password and abide by CWDM policy on password security (see the relevant section on password security).

6.3.13.5 Sensitive confidential material should NOT be sent through the electronic mail system unless it is encrypted.

6.3.13.6 Confidential information should be redirected only where there is a need and with the permission of the originator, where possible.

6.3.13.7 Electronic mail messages can be forged in the same way as faxes and memoranda. If a message is suspect, users should verify its authenticity via telephone or fax.

## 6.4 Guidelines on Passwords

6.4.10 Password Management

6.4.10.1 Passwords should be memorized - never written down.
6.4.10.2 Passwords belong to individuals and must never be shared with anyone else.
6.4.10.3 Passwords should be changed every 30-60 days, or immediately if compromised.

6.4.11 Password Administration

6.4.11.1 New or changed passwords must be given in writing only to the identified user - never over the telephone or via email.

6.4.12 Password Construction

6.4.12.1 Password security isn't just a matter of thinking up a nice word and keeping it to yourself. You must choose a password which will be difficult for someone else to guess or crack. We often have a tendency to forget passwords, so we choose something that has particular relevance to ourselves: the name of a loved one, our favorite car, sport, or ice cream, etc. Anyone knowing a little about us can make a list of these words and easily crack the password. All-digit passwords usually fall into this category - birth dates, phone numbers.

6.4.12.2 Observe the following guidelines when choosing your password:

6.4.12.2.1 A password should be at least 6 characters long.
6.4.12.2.2 NEVER make your password a name or something familiar, like your pet, your children, or partner. Favorite authors and foods are also guessable.
6.4.12.2.3 NEVER, under any circumstances, should your password be the same as your username or your real name.
6.4.12.2.4 DON'T use words that can be associated with you.
6.4.12.2.5 Do not have a password consisting of a word from a dictionary. Most basic cracking programs contain over 80000 words, and plenty of variations.
6.4.12.2.6 Try to have a password with a number or mixed case letters.
6.4.12.2.7 Choose something you can remember, that can be typed quickly and accurately and includes characters other than lowercase letters, e.g. S3ct1On (The word "section" with a mix of numbers and case letters).

## 6.5 Internet Conditions, Standards, and Guidelines

### 6.5.10 Scope

6.5.10.1 The new resources, new services, and inter-connectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this statement describes CWDM official policy regarding Internet security. It applies to all CWDM employees and temporaries who use the Internet with CWDM computing or networking resources, as well as those who represent themselves as being connected with CWDM.

### 6.5.11 Transmission of Information

#### 6.5.11.1 Downloading

6.5.11.1.1 Where permission has been granted for software to be downloaded from non-CWDM sources via the Internet, this software must first be screened with virus detection software prior to being invoked. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

6.5.11.2 Suspect Information

6.5.11.2.1 All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

6.5.11.3 Contacts

6.5.11.3.1 Contacts made over the Internet should not be trusted with CWDM information unless reasonable steps have been taken to ensure the legitimacy of the contacts. This applies to the release of any internal CWDM information.

6.5.11.4 Information Security

6.5.11.4.1 Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, CWDM, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods. Credit card numbers, log-in passwords, and other parameters that can be used to gain access to CWDM systems, networks and services, must not be sent over the Internet in readable form.

6.5.12 Personnel Security

6.5.12.1 Privacy

6.5.12.1.1 Staff using CWDM information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, workers should not send information over the Internet if they consider it to be private.

6.5.12.2 Right to Examine

6.5.12.2.1 CWDM management reserves the right to examine internet logs and usage reports, as provided by the IT department.

6.5.12.3 Public Representations

6.5.12.3.1 All external representations on behalf of the CWDM must first be cleared with the Municipal Manager. Additionally, to avoid libel problems, whenever any affiliation with the CWDM is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited.

6.5.12.3.2 All staff must not publicly disclose internal CWDM information via the Internet that may adversely affect the CWDM's relations or public image.

6.5.12.3.3 Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, and related public postings on the Internet. All related postings must be cleared with the Municipal Manager prior to being placed in a public spot on the Internet.

6.5.12.4 Access Control

6.5.12.4.1 Unless the prior approval of the Manager of the IT Department has been obtained, staff may not establish modems, Internet or other external network connections that could allow non-CWDM users to gain access to CWDM systems and/or networks and CWDM information.

6.5.12.4.2 Likewise, unless the Manager of the IT Department has approved in advance, users are prohibited from using new or existing Internet connections to establish new communication channels e.g. electronic data interchange (EDI) arrangements, on-line database services, etc.

## 6.6 Standards and Guidelines for Strategic Systems

### 6.6.10 Strategic System Platforms

6.6.10.1 Definition of 'Strategic'

6.6.10.1.1 A strategic system is one that meets several of the following criteria:

6.6.10.1.1.1 Is critical to the mission of the CWDM.
6.6.10.1.1.2 Affects large parts of the CWDM.
6.6.10.1.1.3 Yields CWDM-wide benefits.
6.6.10.1.1.4 Is large.
6.6.10.1.1.5 Is expensive.

6.6.10.1.2 Management of Strategic Systems

6.6.10.1.2.1 The following policies apply in the management of strategic systems:

6.6.10.1.2.1.1 Strategic platforms will be managed and operated by the IT Department.

6.6.10.1.2.1.2 Strategic Applications will be managed by the designated custodian of the application.

6.6.10.1.3 Physical Security

6.6.10.1.3.1 The following standards of physical security of strategic platforms must be met:

6.6.10.1.3.2 Premises must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc.

6.6.10.1.3.3 Air temperature and humidity must be monitored regularly.

6.6.10.1.3.4 Platforms must be electrically powered via UPS to provide the following:

6.6.10.1.3.5 Minimum of 15 minutes' operation in the event of a power blackout.

6.6.10.1.3.6 Adequate protection from surges and sags.

6.6.10.1.3.7 Trigger an orderly system shutdown when deemed necessary.

6.6.10.1.4 Physical Access

6.6.10.1.4.1 External doors will remain locked, preferably with electronic locks.

6.6.10.1.5 User Access

6.6.10.1.5.1 New Users

6.6.10.1.5.1.1 New userid's will be handled as follows:

6.6.10.1.5.1.1.1 Written application must be submitted on the appropriate IT Support form.

6.6.10.1.5.1.1.2 The application form must have been signed by someone in authority, e.g. Department Head, Director, etc.

6.6.10.1.5.1.1.3 The applicant must present suitable personal identification.

6.6.10.1.5.1.1.4 The application form will be kept indefinitely by the IT Department.

6.6.10.1.5.1.1.5 The new userid and password will be given orally to the applicant; unless special delivery has been authorized due to special circumstances (e.g. applicant is overseas).

6.6.10.1.5.1.1.6 If the Operating System supports a password aging facility then it must be set to force password change on the first login.

6.6.10.1.5.1.1.7 The access level will be no higher than required as approved by the Department Head.

6.6.10.1.5.2 Terminating Users

- The user IDs of persons leaving the CWDM or no longer requiring access will be disabled.
- The HR Department must inform the IT department of any individuals no longer under the employ of the CWDM.

6.6.10.1.6 Fire Detection and Control

6.6.10.1.6.1 There will be smoke and thermal detectors on the premises.

6.6.10.1.6.2 Underfloor areas will have smoke detectors.

6.6.10.1.7 Data Integrity

6.6.10.1.7.1 Security backups of all data will be made daily.

6.6.10.1.7.2 The backup regime must meet the following criteria:

6.6.10.1.7.2.1 Enable recovery to at least the start of business on any weekday of a failure.

6.6.10.1.7.2.2 Provide at least one more level of backup to a previous time, to cover the case of the failure of the primary backup media.

6.6.10.1.7.2.3 There must be offsite storage of security backup media to enable a full data recovery to no earlier than one working week.

6.6.10.1.7.2.4 There must be a validation of security backup media at least once every 30 days.

6.6.10.1.8 Password Aging

6.6.10.1.8.1 If the Operating System provides the facility, automatic Password Aging will be enforced. The life of a password should be no less than 30 days.

6.6.10.1.9 Disaster Recovery Plan

6.6.10.1.9.1 There will be a Disaster Recovery Plan for every Strategic system.

## 6.7 Standards and Guidelines for Desktop Computers

### 6.7.10 Desktop Computer Security Guidelines

6.7.10.1 Definition

6.7.10.1.1 Desktop computers are personal workstations that, though possibly linked to other computers via a Local Area Network, function as stand-alone units. The terms of the standards and guidelines for desktops will also apply to notebooks.

6.7.10.2 General Obligations

6.7.10.2.1 Users and Department Heads of Desktop computers are subject to the "Conditions of Use" and "Code of Practice" specified in the CWDM IT Security Policy.

6.7.10.3 Hardware Security

6.7.10.3.1 Lock offices. Office keys should be registered and monitored to ensure they are returned when the owner leaves the CWDM.

6.7.10.3.2 Secure Desktops in public areas. Equipment located in publicly accessible areas or rooms that cannot be locked should be fastened down by a cable lock system or enclosed in a lockable computer equipment unit or case.

6.7.10.3.3 Secure hard disks. External hard disks should be secured against access, tampering, or removal.

6.7.10.3.4 Mark personal computers clearly with the name of the owner.

6.7.10.3.5 Locate computers away from environmental hazards.

6.7.10.3.6 Store critical data backup media in a secure off-site location.

6.7.10.4 Access Security

6.7.10.4.1 Utilize password facilities to ensure that only authorized users can access the system. Where the Desktop is located in an open space or is otherwise difficult to physically secure then consideration should be given to enhanced password protection mechanisms and procedures.

6.7.10.5 Confidential Information

6.7.10.5.1 Encrypt sensitive and confidential information where appropriate.

6.7.10.5.2 Monitor printers used to produce sensitive and confidential information.

6.7.10.5.3 Overwrite sensitive files on fixed disks, flash disks, or cartridges.

6.7.10.6 Software

6.7.10.6.1 Software is protected by copyright law. Unauthorized copying is a violation of CWDM Copyright policy. Anyone who uses software should understand and comply with the license requirements of the software. The CWDM is subject to random license audits by software vendors.

6.7.10.7 Viruses

6.7.10.7.1 Computer viruses are self-propagating programs that infect other programs. Viruses and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. Fixes to infected software should be made as soon as a problem is found.

6.7.10.7.2 To decrease the risk of viruses and limit their spread:
6.7.10.7.3 The IT department must approve and check all software before installing it.

6.7.10.7.4 The IT department will use software tools to detect and remove viruses.

6.7.10.7.5 The IT department must isolate immediately any contaminated system brought to the IT department's attention.

6.7.10.8 Computer Networks

6.7.10.8.1 Networked computers may require more stringent security than stand-alone computers because they are access points to computer networks.

6.7.10.8.2 While the IT Department has responsibility for setting up and maintaining appropriate security procedures on the network, each individual is responsible for operating their own computer with ethical regard for others in the shared environment.

6.7.10.8.3 The following considerations and procedures must be emphasized in a network environment:

6.7.10.8.4 It is the responsibility of each CWDM user not to open emails or attachments received from unfamiliar sources as they might contain viruses. Users should also not share their flash disks with other users, or allow other users to connect their flash disks to their PCs or laptops unless such flash disks have been scanned by the IT department for viruses.