VETERINARY MEDICINES DIRECTORATE

INFORMATION COMMUNICATION TECHNOLOGY (ICT) POLICY

Vision

To be the a leading and globally recognized regulatory agency for veterinary medicines, vaccines, and animal health technologies

Mission

To safeguard animal health, human health, and the environment and promote animal welfare by assuring the quality, safety, and effectiveness of veterinary medicines, vaccines, and other animal health technologies.

Core Values

- Professionalism
- Integrity
- Transparency and accountability
- Innovativeness
- Teamwork
- Inclusivity

TABLE OF CONTENTS

ABBREVIATIONS

VMD - Veterinary Medicine Directorate

DRC - Disaster Recovery Centre

ICT - Information Communication Technology

IT - Information Technology

FYI - For Your Information

NDR - Non Delivery Report

FYA - For Your Action

SLA - Service Level Agreement

FTP - File Transfer Protocol

NAT - Network Address Translation

SOE - Standard Operating Environment

DEFINITIONS

Authentication: The process of identifying an individual usually based on a username and password. Authentication is distinct from authorisation, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. Three types of factors are used to provide authentication: a) something you know [e.g. a password], b) something you have [e.g. a certificate or card], and c) something you are [e.g. a fingerprint or retinal pattern]. Using any two in conjunction is known as two-factor authorisation.

BIOS: The Basic Input Output System refers to software code that is designed to always run when a computer is first switched on. It typically tests and initializes system devices so that other software such as the operating system can commence running.

Email: The electronic transmission of information through a mail protocol such as Simple Mail Transfer Protocol (SMTP).

File Transfer Protocol (FTP): A standard Internet protocol that is used to exchange files between computers on the Internet. FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to download programs and other files to your computer from other servers.

Firewall: Security device (either hardware or software based) that is used to restrict access in communication networks. They prevent computer access between networks, or networks and applications, and only allow access to services that are expressly registered. They also keep logs of all activity, which may be used in investigations.

Format: A format involves preparing a storage medium such as a hard disk drive for reading and writing of data. Often, these occur in the form of a 'high-level' format which does not erase any data on the storage medium but simply tests the disk to make sure all sectors are reliable, marks bad sectors and creates new internal address tables that it later uses when new information is written to or access from the disk. A low-level format, conversely, involves the entire storage medium being written with binary zeros which results in the removal of all partitions, clusters, boot sectors and data.

Identification: The process that enables recognition of a user by a system, generally by the use of unique, machine-readable User IDs.

Network: The system established by an Directorate whereby workstations, servers and other data processing nodes are interconnected for the purpose of electronic data communication, storage and processing within and outside the Directorate.

Network Address Translation (NAT): A feature typically employed by firewalls/routers that interface between external and internal facing networks. NAT allows the allocation of multiple IP addresses to machines located in internal networks, without the existence of

these machines being revealed on the external network. Instead, only a single or small number of IP addresses are advertised to the external network, which are then mapped by the router/firewall to the machines on the internal network.

Malicious software: Is any software that is intended to conduct actions without authorisation, including stealing, modifying or destroying data, bypassing access restrictions or hijacking system resources.

Personal Firewall: Refers to a software application, which, like a dedicated hardware firewall device, inspects network traffic passing through it, and denies or permits passage based on a set of rules (for example, based on the software application that is trying to send the traffic from a workstation).

Password: A secret word, sentence, or code used to validate a user's identity to access an information system or service. Passphrase differs from passwords only in length. Passwords are usually shorter (from 8 to 12 characters) while passphrases are usually longer (up to 100 characters and more).

Sensitive Information: Information assets classified as restricted, confidential or for internal use.

Standard Operating Environment (SOE): Refers to a standard implementation within an organisation of an operating system and an associated set of software applications. SOEs are typically implemented using a standard hard disk image that can be deployed across several workstations in an organisation.

System Utility: A specialized program designed for more technical users as a tool, or set of tools for checking the system, housekeeping, monitoring system health status or repairing files.

User: A person or process that is accessing any Directorate information system who has a log-in account on the network.

User ID: A unique character string that is used by a system to identify a specific user. It may also be referred to as username, user account, profile, user profile, login name, or login account.

Viruses: An unauthorized program that replicates itself, attaches itself to other programs and spreads onto various data storage media or across the network. The symptoms of virus infection include much slower computer response time, inexplicable loss of files, changed modification data for files, increased file sizes, and a possible total failure of the infected computer.

Workstation: A personal computer that includes both desktop and laptop/notebook computers used to store information or access information systems of the Directorate.

1.0 Preamble

Information Communication Technology (ICT) has become the backbone of day to day operations in all organizations. VMD is not an exception. While the Board and the management of VMD recognize this fact, organizations all over the world, including VMD are faced with challenges of ICT security and establishment of acceptable use of ICT as well as legal compliance.

This ICT policy document therefore seeks to provide guidelines for compliance, acceptable and secure use of information communication technology by both VMD employees and VMD business partners.

2.0 Objectives

All VMD ICT facilities and information resources remain the property of VMD and not of particular individuals, teams or departments. It is in view of this fact that the objectives of this document are thus to:

- ensure efficient use of ICT resources by VMD employees and affiliates;
- ensure availability of ICT systems;
- ensure information security of VMD systems;
- ensure the spirit of awareness, co-operation, trust and consideration for others.
- ensure compliance with the Laws of Kenya;
- Improve speed and quality of service delivery to customers and other stakeholders.

3.0 Scope

The ICT policy document relates to all Information Technology facilities and services provided by VMD including, but not limited to, email system, databases, operating systems, internet, telephone systems, wireless communication, peripherals, printers and copiers. All VMD employees, volunteers as well as business partners are expected to adhere to it. This document shall be effective from the date of approval.

4.0 Precautionary and Disciplinary Measures

Deliberate and serious breach of the policy statements in this section will lead to disciplinary measures which may include the offender being denied access to computer facilities.

4.1 Copyright

Not taking care to use software legally in accordance with both the letter and spirit of the relevant licensing and copyright agreements is illegal and may result in criminal charges.

4.2 Security

4.2.1. No attempt shall be made to gain unauthorized access to information or facilities. It is an offence to obtain unauthorized access to any computer (including workstations and PCs) or to modify its contents. In the event that one does not have access to information resources needed, the IT Support team should be contacted for assistance.

4.2.2 Don't disclose personal system passwords or other security details to other staff, volunteers or external agents and don't use anyone else's login; this compromises the security of VMD. If someone else gets to know your password, ensure you change it or get IT Support to help you.

4.2.3. If you leave your PC unattended without logging off or locking the session, you are responsible for any misuse of it while you're away. The ICT Officer shall configure the workstations to lock after a certain duration.

4.2.4. ALWAYS check flash disks for viruses even if you think they are clean (Contact ICT officer). Computer viruses are capable of destroying VMD information resources. It is better to be safe than sorry.

4.3. Information about people: If you are recording or obtaining information about individuals, make sure you are not breaking Data Protection legislation (The ICT officer can guide on this.)

4.4. You are a representative of VMD when you are on the Internet:

4.4.1. Make sure your actions are in the interest (and spirit) of VMD and don't leave VMD open to legal action (e.g. libel).

4.4.2. Avoid using the Internet for purposes of trading insults with other people whom you disagree with.

4.4.3 **Obscenities/Pornography:** Don't write it, publish it, look for it, bookmark it, access it or download it.

4.5 **Electronic Espionage:** Any information available within IT facilities must not be used to monitor the activity of individual staff in any way (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files etc.) without their prior knowledge. Exceptions are:

(i) In case of a specific allegation of misconduct, Management Team can authorize accessing of such information while investigating the allegation. This may necessitate disabling the victim from accessing IT facilities pending investigation.

(ii) When the ICT Officer cannot avoid accessing such information whilst fixing a problem. The person concerned will be informed immediately and the information will not be disclosed wider than is absolutely necessary.

5.0 Asset Management

This establishes a framework for the management and control of VMD ICT assets. It ensures that equipment and infrastructure planning and subsequent asset administration procedures are cost effective, efficient, transparent and that all steps in the responsibility chain are well documented, understood and executed. These steps involve acquisition, the proper recognition, measurement, accounting, safeguarding and disposal of Assets.

-It covers the end-to-end management of all ICT assets at VMD. It details the policies, processes, roles and accountabilities for:

- identifying the needs for asset procurement including budgeting and financing
- Asset receipt and commissioning
- asset utilization and security
- asset maintenance and repairs
- maintaining asset registers and reporting
- asset disposal

5.1 Purchasing is only one option to have access to assets

The decision to purchase an asset should be made after other options have been considered such as renting. Purchase is based on well-established need and other factors (total cost of ownership per year, ease of maintenance, ease of use, etc.).

5.2 Asset receipt and commissioning

All assets (where practicable) will be received by the ICT Officer until certified ready for allocation to a user. Some items may require storage while waiting for installation or commissioning or configuration, while others are ready for use on delivery.

Items that require configuration before issue e.g. computers will be kept safely and handed over to the final user once ready.

The ICT Officer will:

- Inspect assets for quality and physical condition.
- Certify on the Goods Receiving Note (GRN) that the assets delivered/ installed meet specifications in the delivery order/packing list, purchase order (PO) and any other contract document. The GRN will be sent to the Accounts Office for payment of the invoice.

- Ensure that third party test/inspection certificates, warranty and other Quality Assurance documents where appropriate, are received together with the materials.
- Ensure safe storage to the required location.
- Ensure the custodian is fully trained and skilled to use the equipment properly.

5.3 Asset utilization and security

Custodians are personally responsible for assets under their control and so are users if they are not the custodians. Technical units who handle assets under repair are also responsible for the security of the assets.

Custodians and/or users, depending on circumstances, are liable for any loss or damage. Examples of negligence:

- An employee leaves an VMD laptop unattended while they travel.
- An employee deviates from proper procedures to operate a piece of laboratory equipment although they have been fully trained on using the equipment.

The safeguarding of equipment such as laptops and digital cameras is particularly important because of their attractive and portable nature but also because of the confidential information that they may contain. Steps that can be taken include but are certainly not limited to:

- Keep your office drawers locked when unattended and when travelling
- Do not leave items unattended in public places (e.g. airports, airplanes)
- Do not leave items unattended in vehicles
- Always clearly label items to deter theft
- Transport laptops in secure bags or cases
- Do not flaunt cameras or cellphones in public places
- Back up data on other storage devices

Custodians for assets managed in a pool have to ensure that the assets they are responsible for are always securely kept. Specially designed cabinets exist for laptops for instance and could be used if there is no effective alternative.

When an asset has been officially handed over to the ICT Officer for maintenance or repair, the responsibility for the security of the asset rests with the ICT Officer. The ICT Officer should take measures such as secure cabinets or other devices to ensure the security of the assets at all times while under their care.

Directorate security officials may question individuals removing equipment. Staff transporting equipment should be prepared to present a written authorization from the ICT Manager. For items that are frequently taken out of the VMD compounds such as laptops, the ICT Officer should keep a running list of staff allowed to take their laptops out of the VMD compound and the relevant information on the laptop.

In case of theft or damage to the ICT equipment, the ICT Manager is to be notified by the ICT Officer immediately of cases of theft or malicious damage of VMD assets. The Directorate will launch investigations into the loss of the asset and a written report covering all relevant matters and make recommendations by the ICT Officer.

In case negligence is established the Directorate will, if necessary take any or a combination of the following actions:

- Recover replacement cost of item from staff salary/ dues.
- Temporarily suspend staff implicated in the report pending investigations.
- Recommend dismissal of staff whose responsibility is clearly established.
- Refer the matter to the police for further investigation.

5.4 Maintenance and repairs of assets

All equipment are included in a regular and appropriate maintenance plan managed by the ICT Officer. The equipment should be maintained in good working order by care and servicing. The most efficient repair and maintenance strategy is to be established and adopted. Preventive maintenance is a vital part of the plan.

The ICT Officer will maintain a replacement and maintenance plan. The plan should indicate

- Asset identification details (e.g. serial number)
- Year of purchase
- Current condition
- Maintenance details (costs, frequency, provider)
- Suggested disposal date

5.5 Asset monitoring, recording and control

The Directorate must have systems in place for accurately recording and monitoring transactions related to ICT equipment on a timely basis and for safeguarding the assets from fraud or misappropriation. The asset registers must be updated in a timely manner and contain relevant, accurate and sufficient information.

5.6 Asset Disposal

Asset disposal, or retirement or sale is the removal from usage of a capital asset or part thereof when the asset is sold, dismantled, abandoned or otherwise disposed of.

5.6.1 Decision to dispose

Assets for disposal will be identified on an on-going basis and systematically at least once a year. Recommendations to dispose of assets can be made by the user, the ICT Officer or

other relevant stakeholders. The ICT Manager may recommend the method of disposal. Completed forms will be submitted to the ICT Manager who will ask the ICT Officer to prepare a summary list of all assets and all relevant information and call for a meeting of the Disposal committee.

The ICT Officer may start the process for disposal by completing an **Asset disposal form** for the old asset.

5.6.2 Who is involved and when?

Once the decision to dispose of an item is made:

- The ICT Manager coordinates the disposal process by convening the necessary meetings of the Disposal committee and providing the necessary information.
- The Disposal committee will make a decision for each item listed on the report and decide on other relevant information (e.g. disposal method, reserve price). The summary sheet should be signed by the committee and forwarded to the Chief Executive Officer who will confirm compliance with VMD policies before approving/forwarding.

5.6.3 Documentation of disposal

An "**Asset Disposal Form**" must be completed once the disposal has been effected.

All minutes of the disposal committee must naturally be carefully kept as well.

5.6.4 Disposal methods

These include:

- Donations
- Auction
- Private sale - In case an auction is not the most efficient way (e.g. for scrap), a private sale can be organised to the highest bidder among three offers from professional scrap sellers.
- "Cannibalization"
- Theft (unfortunately possible!)

The disposal details will be entered on the **Asset Disposal Form.**

5.6.5 General disposal process

The Disposal committee must ensure that the process follows asset disposal guidelines detailed below and that the sale promotes and protects VMD's interests at all times. The committee will also oversee the auction/ bidding process and decide on any queries and

issues that may be raised by auction participants. All meetings will be minuted. The principles to be applied are as follows:

- **Individual asset or lot**
  Sales will usually be organized for individual assets. It may be practical in certain circumstances to constitute lots to facilitate the sale process.

- **Reserve price**
  All sales will have a reserve price either by individual item or by lot. The relevant Officer will, after having established the best estimation of market price by means of at least two trustworthy and documented valuations, recommend a reasonable reserve price for the vehicle to the Disposal Committee.

  In arriving at the reserve price for assets that may not have a clear market value, they will take into consideration the assets' current market value, the book value and the physical condition. The reserve price will be advertised.

- **Bidding process and deposits**
  Offers to staff will be invited through internal advertisements while for the public; a newspaper of wide circulation will be used. It should be made clear to potential bidders that the sale is on a "as is, where is" basis. Interested bidders will be required to provide the following in a sealed envelope.
  - Name and telephone number
  - Lot number of the asset being bid for
  - Description of asset being bid for
  - Bid amount

All bids, whether by staff or members of the public, will be dropped in a designated tender box to be opened by the Committee after the given deadline.

The committee will do the bid analysis and recommend award to the highest bidder above the reserve price.

Unsuccessful bidders will be refunded their deposit in full within 2 working days from the award date. Bidders who are successful and do not complete the payment process for the balance within two calendar weeks will be fined a set amount and the balance refunded, and the asset offered to other bidders.

6.0 Website Management

The website is managed and operated by the ICT Officer and any external web developer or search engine optimization team to handle, control or produce any of the website

content. All contributions, amendments and graph VMD / images are created by the ICT Officer and the external website developer and uploaded.

Third party website developers are employed by VMD to develop and host the website. Appropriate agreements are in place to ensure optimum quality control measures.

The materials contained on the above website are deemed to be for general information purposes only and do not constitute legal or professional advice.

6.1 Responsibility

The ICT Manager or ICT Officer has responsibility for the management of the website including:

- Ensuring content is up to date;
- Ensuring content does not infringe copyright;
- Specifying conditions for downloading material;
- Overseeing linking arrangements;
- Ensuring posting of a privacy notice explaining how any data collected from visitors will be managed by the Directorate.

The Chief Executive Officer may delegate responsibility for inputting and maintaining the website however accountability for any content that is shown on the website remains with the ICT Manager.

6.2 Copyright and Trademark Notices

The contents of the site are protected by copyright under international law. Users are permitted to read the contents of our website and make copies of such content for their own personal use. They may also give copies to colleagues for their personal use on terms that VMD is acknowledged as the source, the text is not altered in any way and the attention of the recipients is drawn to this warning. All other use and copying of any of the contents of this site is prohibited. Copying from websites of third parties is subject to any requirements applicable to those sites.

6.3 Links to Third Party Sites

This website may include hyperlinks to websites operated by other parties. VMD is not responsible for examining or evaluating them and their inclusion does not imply

endorsement of their content. VMD does not receive any fee from any website owner who may be cited or linked to from the website. All external links should be considered for information only purposes.

6.4 Accessibility

We are committed to making our website accessible for all our website visitors.
We are committed to providing an accessible web service. If you experience problems or have any suggestions for improvement, please contact the ICT Manager or ICT Officer.

6.5 Data Protection

This Website is owned and operated by VMD, who is the 'Data Controller' for the purposes of the Data Protection Act 2013. This document is intended to explain how we use the information we collect, how a client can instruct us if they prefer to limit the use of that information, and the procedures we have in place to safeguard their privacy.

6.6 Collection, Utilization and Security of Data

Without limitation, any of the following Data may be collected:

6.6.1 Name;
6.6.2 Gender;
6.6.3 Contact information such as email addresses and telephone numbers;
6.6.4 Address and post code
6.6.5 Financial information such as credit / debit card numbers; (for those using our online payment facility)
6.6.6 IP address (automatically collected);
6.6.7 Web browser type and version (automatically collected by web analytics and traffic analysis software);
6.6.8 Operating system (automatically collected by web analytics and traffic analysis software);

6.7 Our Use of Data

Any personal data will be retained by VMD for as long as the client needs access to the Services and Systems provided on the Website or the client has otherwise agreed (opted in) to.

Unless we are obliged or permitted by law to do so, clients Data will not be disclosed to third parties without their express permission. This includes our affiliates and/or other companies within our group.

All personal Data is stored securely in accordance with the principles of the Data Protection Act 2013.

Any or all of the above Data may be required by us from time to time in order to provide the client with the best possible service and experience when using our Web Site. Specifically, data may be used by us for the following reasons:

- internal record keeping
- improvement of our products / services
- transmission by email of promotional materials that may be of interest to the client
- contact for market research purposes which may be done using email, telephone or mail. Such information may be used to customize or update the website.

We use anonymous cookies to make this site as useful as possible. They are small text files we put in your browser to track usage of our site but they don't tell us who you are.

6.8 Cookie Policy

VMD may collate and use information about visitors to this website. Some of this information will include the use of cookies. Cookies also known as browser cookies or tracking cookies, are small often encrypted text files located in browser directories. They are used by web developers to help users navigate their websites efficiently and perform certain functions. The cookies in use on this website owned and managed by VMD gather information and statistics about visitors. Cookies make it easier for you to access our content pages and to log on to any user accounts which we create for you. We do not use or store personal data without express permission and use cookie related data on a collective basis to analyse traffic and website performance. We use this information to help us improve our websites.

You can change the settings on your web browser to refuse cookies, or you can enable the browser to see your consent for each cookie it detects. You can find out how to do this by clicking "help" on your browser menu.

6.9 Liability

The material displayed on our site is provided without any guarantees, conditions or warranties as to its accuracy. The content on our website is deemed to be for general information purposes only and should not constitute legal or professional advice. VMD accepts no responsibility for any loss which may arise from accessing or relying upon on information contained in this website.

7.0 Email

7.1 When to use email:

7.1.1. Use it in preference to hard copy with the aim of reaching people quickly (saving time on photocopy/distribution) and to help reduce paper use. Think and check messages before sending (just as you would a letter or a paper memo).

7.1.2. Use the phone (including voicemail if no reply) for urgent messages (email is a good backup in such instances).

7.1.3. Use VMD intranet (not email) to communicate all relatively static information (e.g. policy, procedures, briefing documents, reference material and other standing information). Record information on the intranet in a well-structured manner (consulting with the ICT Manager or ICT Officer as appropriate). Use email merely as a pointer to draw attention to new and changed information on the intranet.

7.2 Use of Distribution Lists

7.2.1 Only send email to those it is meant for; don't broadcast (i.e. send to large groups of people using email aliases) unless absolutely necessary since this runs the risk of being disruptive. Unnecessary (or junk) email reduces computer and network performance and wastes disc space.

7.2.2 Use the standard aliases for work related communication only. Email aliases are pre-defined 'shortcuts' for distributing internal emails to specific groups of people. Systems administrators can tell you what these are and how to use them.

7.2.3 If you wish to broadcast other non-work related information or requests (e.g. information or opinions on political matters outside the scope of VMD, campaigning, social matters, personal requests for information etc.) it is better to use a Webmail account or a personal email account at home; don't use the standard (work) aliases. Webmail accounts are personal email accounts that are stored on the Internet and can be accessed from anywhere with a standard browser, e.g. home or cybercafé. IT Support can advise you on setting up such an account.

7.2.4 Keep VMD internal email aliases internal. If you are sending an email both to VMD alias and outside of VMD use the alias as blind carbon copy (i.e. the bcc address option) so that the external recipient does not see the internal alias.

7.2.5 Don't broadcast emails with attachments to large groups of people. The stop gap should be 20 MB- either note in the email where it is located for recipients to look, or include the text in the body of the email. Failure to do this puts an unnecessary load on the network.

7.3 General points on email use

7.3.1 When publishing or transmitting information externally be aware that you are representing VMD and could be seen as speaking on behalf of VMD. Make it clear when opinions are personal. If in doubt, consult the Chief Executive Officer.

7.3.2 Check your inbox/in-tray at regular intervals during the working day. Keep your in-tray fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical).

7.3.3 Keep electronic files of electronic correspondence; only keeping what you need to. Don't print it off and keep paper files unless absolutely necessary.

7.3.4 Use prefixes in the subject box whenever appropriate.

7.3.5 Treat others with respect and in a way you would expect to be treated yourself (e.g. don't send unconstructive feedback, argue or invite colleagues to publicize their displeasure at the actions/decisions of a colleague).

7.3.6 Don't forward emails warning about viruses (they are invariably hoaxes and ICT officer will probably already be aware of genuine viruses- if in doubt, contact the ICT Officer for advice) Exception: Only ICT officer can forward warnings about viruses.

7.3.7 Members of staff to be issued with an official email address and if they leave, have it deactivated after a month.

7.3.8 Email addresses to be custom made to VMD e.g. First initial plus last name.

7.4 Email etiquette

7.4.1 Being courteous is more likely to get you the response you want. Do address someone by name at the beginning of the message, especially if you are copying another group of people.

7.4.2 Make your subject headers clear and relevant to your reader(s) e.g. don't use subject headers like "stuff". Don't send a subject header of, say "accounts" to the accountant.

7.4.3 Try to keep to one subject per email, especially if the content is complex. It is better for your reader(s) to have several emails on individual issues, which also makes them easy to file and retrieve later. One email covering a large variety of issues is likely to be misunderstood or ignored.

7.4.4 Using asterisks at each end of a word (e.g. *now*) is common practice of highlighting text.

7.4.5 Capitals (e.g. NOW) can also be used to emphasize words, but should be used sparingly as it is commonly perceived as 'shouting'.

7.4.6 Don't open an email unless you have a reasonably good expectation of what it contains and its source, e.g. Do open report.doc from an Internet colleague you know, don't open explore.zip sent from an address you've never heard of, however tempting. Alert IT Support if you are sent anything like this unsolicited. This is one of the most effective means of protecting VMD against email virus attacks.

7.4.7 Keep email signatures short. Your name, title, phone and website address may constitute a typical signature.

7.4.8 Understand how forwarding an email works. If you forward mail, it appears (to the reader) to come from the originator (like passing on a sealed envelope). If you forward mail and *edit it* in the process, it appears to come from you- with the originator's details usually embedded in the message. This is to show that the original mail is no longer intact (like passing on an opened envelope)

7.5 Delivery and Receipt of Mails

The nature of emails is controversial; as while a certain mail may be SPAM to one person it may not be SPAM to another. There are lots of SPAM filtering software out in the market, but none is perfect. There are always cases of some mails being passed out by the software as being clean while it is not clean *(false positives)* or being rejected as SPAM while it is not SPAM *(false negatives).* This controversy is further complicated by the fact that there are many parties involved in a mail.

For a mail to be successfully delivered, it entails that:

1. The sender uses the correct address;
2. The internet of the sender is up;
3. The internet of the recipient is up;
4. That the sender's organization server has no technical problems;

5. That the recipient's mail server has no technical problems;
6. That the sender's PC is online;
7. That the recipient's PC is online; and
8. That the anti-spam software recognizes it appropriately.

It is due to this complexity that urgent mails should be given at least 15 minutes for delivery and a follow up made through telephone. Users receiving NDR (Non-Delivery Reports) for mail failures shall forward the same to ICT Person for troubleshooting. Staff are however required to ascertain, before launching a complaint that the address of the recipient is correct and free from typos.

Complaints about mail receipt failure should always be accompanied by the sender address and the recipient address. This will enable the ICT Officer to narrow down to the particular case and give a report and advice to the affected user, soonest possible (within 30 minutes)

8.0 Internet

The purpose of this is to establish security measures to ensure a sufficient level of protection is provided in response to the security risks presented by Internet use within the Directorate.

The Internet provides access to an array of information, resources and services that provide potential opportunities and benefits which aid and support the work of the Directorate. However, if Internet use within the Directorate is not securely managed, it can expose the Directorate to risks at both a technical level (with potential damage being caused to ICT infrastructure) and an operational level (with misuse of Internet resources leading to possible reputational damage to the Directorate and a loss in productivity).

It also covers the responsibilities of users with regard to Internet security controls but it does not cover the matter exclusively. Other Directorate policies, best practice guidelines, standards, and procedures may also define additional responsibilities, especially in regard to network and server security issues.

This policy applies to all permanent and temporary staff within the Directorate as well as contractors and visitors who work and/or visit the Directorate who have a stake in any changes occurring in the Directorate's ICT Service environment.

7.1 Administration of Internet Access

8.1.1 Only authenticated users should have access to the internet from the internal networks.

When using web pages that require a user ID and password for access, it is recommended that staff do not use the same ID and password as is used for access to any internal systems, networks or applications with the Directorate.

All outbound Internet traffic should pass through a web filtering gateway. Access to sites categorised as being potentially harmful to the Directorate will be blocked. Exceptions can be configured upon a written email request to the ICT Officer if the sites have been incorrectly categorised or if required for work purposes.

All Internet traffic (inbound and outbound) should pass through an anti-virus gateway. At a minimum, up-to-date anti malware software should be installed and running on Directorate workstations with Internet connectivity.

The following guidelines apply specifically to Internet facing firewalls:

- Logging of all firewall related activities (including maintenance activities) should be performed at all times.
- An explicit "deny all" rule should be implemented as the last rule in the filtering configuration of Internet facing firewalls to allow for logging of rejected connection attempts to any relevant Internet services.
- Backup firewall configuration files stored offline should only be viewable by designated ICT staff.

The Directorate should establish the standard Internet services to be provided to users, such as:

- Email
- Internet Browsing
- Access to the Directorate's website

A log should be created that records all requests (both inbound and outbound) for Internet services. The generated audit logs should be reviewed on a daily basis by the designated ICT staff of the Directorate to determine if there is any misuse and the same reported to the ICT Manager for disciplinary action.

All FTP and SSH sessions, whether to servers hosted externally or hosted by the Directorate should be logged and monitored.

Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, playing computer games, social media and browsing the Internet) is permitted so long as such use does not:

- incur specific expenditure for VMD;
- Impact on performance of the member of staff's job (this is a matter between each member of staff and their manager);
- break the law; and
- Bring VMD into disrepute.

Other users can browse after working hours and during weekends. Users shall not assume any privacy while browsing the internet.

9.0 Network Security and Access

9.1. Firewalls and Intrusion Detection systems shall be used across the entire VMD network to monitor and prevent hackers, viruses and worms including all other forms of attack. The ICT officer shall ensure that this policy is adhered to. Failure to do this may necessitate disciplinary action depending on circumstances and the management's approval.

9.2. All computers hooked into the network shall mandatorily have an up-to-date anti-virus software to prevent viruses and all other forms of malicious code. Additionally, the computers must have all unnecessary services e.g. disabling certain processes to prevent intrusion. It shall be the responsibility of the ICT Officer to ensure this policy is adhered to, failure to which disciplinary action shall be executed as per the management's approval. All staff are expected to seek authority from the ICT Officer before hooking any laptop to the network. Staff are also expected to timely report outdated versions of antivirus for action to ICT Officer. Failure to do so may result into disciplinary action.

9.3. All servers shall likewise have anti-virus and a form of monitoring to ensure that only authorized users have access. The ICT Officer shall enforce this policy, failure to which disciplinary action may be taken against him/her depending on the circumstances and management's approval.

9.4 Termination of User Access

The main principles are that: access to the Directorate networks should be removed as soon as a user is no-longer eligible to receive these privileges. Access to information and network resources should be transferred to another responsible user if it is still required by the Directorate.

9.4.1 In case of voluntary or scheduled termination of employment of a user, the Directorate should immediately disable the User ID upon the departure of the user to remove their access to the network, unless extension of the account is required for Directorate purposes. In cases where extension is required, authorisation is required from the ICT Officer and the ICT Manager and should not exceed a period of one (1) month.

9.4.2 In case of a user being subject to involuntary termination of employment for cause, the Directorate should disable the User ID, and access to the network, immediately that the decision on termination is made.

9.4.3 Redundant User IDs (i.e. an account of a staff member who has left the Directorate) should not be re-used by other users. After a user has left, their User ID should be deleted and any information or privileges attached to that account removed or transferred to another User ID.

10.0 ICT Hardware and Software

The purpose of this is to communicate the Directorate's policy on workstation security that has be put in place to minimise loss, damage or compromise of ICT assets and interruption to Directorate activities.

Staff are expected to use the ICT hardware and software. Irresponsible/excessive use of the hardware and software for personal purposes is discouraged, and may, depending on the management's determination and approval lead to disciplinary action which may include, but not limited to, denial of service.

10.1 Workstations

This covers the protection of workstations and data from loss, security threats, environmental hazards, and opportunities for unauthorized access. It includes general security controls on Directorate's workstations, virus and threat prevention, workstation maintenance, reassignment and disposal.

10.2 **Workstation Operating Environment**

10.2.1 Standard specifications should be maintained for the procurement of workstations. Purchases of workstations that differ from the standard specifications can be made where a valid business case exists and with the approval of the ICT Manager An inventory of workstations used on the Directorate's network should be maintained.

10.2.2 Notebook computers should be secured.

10.2.3 Workstations should not be taken out of the Directorate premises without an authorized pass.

10.2.4 Workstations, especially notebook computers that are taken out of the Directorate premises should not be left unattended or in left unsecured in locations that increase the risk of theft (e.g. in vehicles or hotel rooms).

10.3 **Workstation Configuration**

10.3.1 A standard configuration for workstations will be maintained. Exceptions to the standard configuration can be made where a valid business case exists and with the approval of the ICT Manager

10.3.2 All necessary operating systems service packs, system patches and hotfixes should be up to date before deployment.

10.3.3 Workstations should be kept up to date through the automated installation of the latest service packs, operating system patches and hotfixes. ICT will regularly monitor to ensure that all workstations have been updated correctly.

10.3.4 Anti-virus software should be installed on all workstations before deployment. They should be actively managed to ensure that the latest software updates and virus signatures are installed. The anti-virus library definitions should be automatically updated at least once per day.

10.3.5 A list of standard software that may be installed and run on workstations will be maintained. Acquisition and use of software that is not included in the standard list can be made where a valid business case exists.

10.3.6 Local administrator privilege should not be configured on Workstations. An exception can be made where a valid business case exists and with the approval of the ICT Officer (e.g. for a notebook user who travels and needs to change configuration).

10.3.7 The workstation's BIOS should be configured to boot from the local hard drive, and prevented from booting from CD or other devices.

10.3.8 Where information classified as confidential or sensitive is kept on the workstation a BIOS password should be set and the hard disk should be encrypted to improve protection of the information.

10.3.9 Notebook computers should have a tracking application installed to deter theft and improve the possibility of recovering lost or stolen equipment. Where information classified as confidential or sensitive is kept on the notebook computer the option to remotely delete data from the hard disk should also be installed.

10.3.10 Workstations should be configured to automatically lock the computer and run a screensaver application after ten (10) minutes of inactivity.

10.3.11 Personal firewall software should not be activated on workstations connected to the internal Directorate networks.

10.3.12 Personal firewall software should be activated on workstations that have Internet access and are outside the Directorate's internal network.

10.3.13 Any unused system utilities, local services and processes in the operating system should be disabled.

10.4 **Workstation Use**

10.4.1 An authorized user is assigned as custodian of each workstation. The custodian takes responsibility for use of the workstation by themselves and any other person.

10.4.2 Transfer of a workstation to another physical location or to a different custodian should follow the procedures set out in the Directorate's asset management procedures.

10.4.3 Workstations that contain sensitive data should be subjected to a low-level format before the workstation is transferred to different custodian.

10.4.4 Users should not install any software or hardware that could potentially be used to compromise the security of workstations, unless there is a legitimate business purpose for this. These might include password hacking tools, network discovery or packet capture tools, and the like.

10.4.5 When a workstation is not in use it should be 'locked', thereby ensuring a password is required to access the workstation again.

10.4.6 When users have finished using a workstation, they should either log off or shut down the workstation.

10.4.7 All workstations connected to the Directorate's networks, either directly or via remote access, should have effective and up-to-date virus protection measures in place.

10.4.8 Workstation users should not disable or otherwise modify the behaviour of installed anti-virus software used on workstations.

10.4.9 Workstation users should not intentionally install, run, copy, store, distribute or develop any form of malicious software code.

10.4.10 Workstation users should not install any software or hardware used to circumvent the Directorate's ICT Security policies. These might include password hacking tools, decrypting tools and discovery tools.

10.4.11 When software is no-longer required it should be removed from the workstation.

10.4.12 Removable media such as USB storage devices should be securely erased and/or formatted when the stored data is no longer required for business purposes.

10.5 **Workstation maintenance**

10.5.1 All repairs and servicing of workstations such as installing/reinstalling/uninstalling and configuring/reconfiguring should be performed the ICT Officer.

10.5.2 When sensitive data exists on internal or external drives that need to be serviced, the data shall be removed in a secure manner (e.g., destruction), to ensure it is unrecoverable and may not be retrieved by any party working on the equipment. Appropriate backup shall be maintained when necessary.

10.5.3 If a storage device that has failed needs to be recovered by a third party data recovery specialist, a non-disclosure agreement will be obtained from the recovery specialist.

10.5.4 When workstation maintenance by a third party has been completed, the ICT Officer shall immediately scan the workstation for viruses and malicious code. The custodian will be responsible for changing all passwords that might have been compromised.

10.6 **Workstation Disposal, Data and Software Removal**

10.6.1 Workstations that are no-longer required for use within the Directorate will be disposed of in accordance with the asset management procedures.

10.6.2 All licensed software should be removed from a workstation before disposal and made available for use on new equipment.

10.6.3 Workstations should be subjected to a low-level format before they are sent for disposal. This is to ensure that no confidential data is compromised and no data remaining on the workstation exposes the recipient to charges of inappropriate usage.

10.6.4 Only software that was installed on the workstation at the time of purchase and is not required for use on another Directorate workstation should be re-installed on the workstation before disposal (e.g. operating system). The software should be configured with the default installation configuration that should not contain any details from of the customised Directorate configuration.

10.6.5 When disposing of removable media such as CD-ROMs or USB drives that contained sensitive data media should be securely erased and/or formatted and then destroyed by breaking the media to prevent further use.

11.0 Passwords

11.1. Do not disclose your password to anyone.

11.2. Do not write it down

11.3. Your password should be a combination of alphanumeric and special characters (! _? $^*#), i. e complex, but easy to remember.

11.4. Passwords must be at least six (6) characters.

11.5. Users are required to change their passwords at least every three months.

11.6. Passwords shall lock for every three unsuccessful attempts

11.7. The maximum number of sessions per user shall be three (3).

11.8. Password Management

11.8.1. This shall be the responsibility of the ICT Officer and/or his appointee(s).

11.8.2. A user whose password has expired, or account locked shall (upon request through the ICT Officer) be assigned another password. The affected user must change the initial password immediately for security reasons; bearing in mind that users are solely responsible for actions committed using their own accounts.

12.0 ICT Related Training

12.1. Every department shall identify training needs at the beginning of every financial year and forward them to the ICT Officer.

12.2. The ICT Officer shall analyze the trainings relevant for every person to make sure that the training requirements are relevant to various department staff and within budget then forward the names and requirements to the ICT Manager

12.3. The Chief Executive Officer shall consider, approve and implement.

13.0 ICT Disaster Recovery

ICT Disaster recovery shall be carried out as outlined in the ICT Services Disaster Recovery Plan. The policy is important and need to secure data/documents in case of any eventualities.

ICT officer to do a backup on all documents in a particular folder on my document on a weekly basis.

14.0 ICT Technical Assistance Request and Complaints

All ICT technical assistance requests and complaints shall be channeled to the ICT Officer. A helpdesk email account or/and software will be used for technical assistance requests and complaints where customers can log in seeking for support.

15.0 Miscellaneous

15.1 Installing Software: Get permission from the ICT officer before you install any software (including public domain software) on equipment owned and/or operated by VMD.

15.2 Data transfer and Storage on the network:

15.2.1 Keep master copies of important data on your profile. E.g. My Documents folder. Otherwise it will not be backed up and is therefore at risk. This applies to staff. If you

change your computer, you should inform the ICT officer to update which facilitates backup to your profile. Personal files should be kept to minimum.

15.2.2 Ask for advice from the ICT Manager of ICT Officer and/or IT Administrators if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disc space very quickly and can bring your network to a standstill.

15.3.3 Be considerate about storing personal (non-VMD) files on VMD network.

15.4 Care of equipment:

- Don't re-arrange how equipment is plugged in (computers, power supplies, network cabling, modems etc.) without first contacting the ICT Officer.
- Don't take food or drink into rooms which contain specialist equipment like servers. Access to such rooms is limited to the ICT Officer and other authorized staff.

16.0 Revision

This policy shall be revised on a yearly basis. Changes necessitating revision shall include changes in technology, statutory regulations and any other reasons as may be determined from time to time by the manager in charge of ICT.

APPROVED BY THE BOARD ON THIS DATE.....25th.....of.....July..... 2025

SIGNED BY	SIGNATURE
CHIEF EXECUTIVE OFFICER	.....
BOARD CHAIR	.....

ANNEX 1: ASSET DISPOSAL FORM

	ASSET DISPOSAL FORM *To be filled whenever an asset is donated or otherwise disposed of*

ASSET DETAILS					
Section 1- To be filled once the asset is disposed off					
Filled by		Signature		Date	
Asset Tag #		Asset Description			
Make and Model		Serial Number			
Decommissioning date					
Reason for disposal					
Method of disposal ☐ Donation to: ..... ☐ Auction ☐ Private sale ☐ Cannibalization ☐ Theft ☐ Other : (Please specify)					
Authorization of the ICT Manager: Name, signature and date					
Authorization of the disposal: Name, position, signature and date					
Confirmation of the disposal : Name, signature and date					
Section 2- To be filled when the asset is sold					
Name of buyer					
Original Cost		Department		Net Book Value	
Proceeds		Gain (Loss)			
Received by Accountant : Name, signature and date :					