A. Policy Management

Document Title:	ICT Policy
Document author:	DGS Operations:
Date approved:	
Effective date:	
Approved by:	NEC
Revision:	Edition 2

B. Revision history

Revision number	Revision date	Revision notes	Owner

C. Acronyms and abbreviations

Acronym / abbreviation	Meaning
GS	General-Secretary
DGS	Deputy-General Secretary
ISO	International Organisation for Standardisation
SNMP	Simple Network Management Protocol
LDAP	Lightweight Directory Access Protocol

D. Definitions

Term	Description
None	

TABLE OF CONTENTS

1. Laptop Security Policy

1.1 Purpose

This policy describes the controls necessary to minimise information security risks affecting DENOSA laptops.

1.2 Introduction

All DENOSA computer systems face information security risks. Laptop computers are an essential business tool but their portability makes them particularly vulnerable to physical damage or theft, either for resale (opportunistic thieves), or for the information they contain (industrial spies). Furthermore, the fact that they are often used outside DENOSA's premises increases the threats from people who do not work for DENOSA and may not have DENOSA's interests at heart.

Do not forget that the impact of a device being stolen is not merely the replacement value but the value of any sensitive data stored on it and the ability in some instances to access the valuable data/ systems through the device. We depend very heavily on our computer systems to provide complete and accurate business information when and where we need it. The impact of unauthorised access to, or modification of, important and/or sensitive data far outweighs the cost of the equipment itself.

1.3 Scope

This policy refers to certain other/general information security policies, but the specific information given here is directly relevant to laptops and, in case of conflict, takes precedence over other policies.

1.4 Policy Detail

1.4.1 Physical security controls for laptops

i. The physical security of ‘your’ laptop is your personal responsibility so please take all reasonable precautions. Be sensible and stay alert at all times.

ii. Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a few seconds to steal an unattended laptop.

iii. If you have to leave the laptop temporarily unattended in the office, meeting room or hotel room, even for a short while, use a laptop security cable or similar device to attach it firmly to a desk or similar heavy furniture. These locks are not very secure but deter opportunistic thieves.

iv. Lock the laptop away (out of sight) when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the boot or glove compartment but it is generally much safer to take it with you.

v. Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. Don’t drop it or knock it about! An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.

vi. Keep a note of the make, model, serial number and the DENOSA asset label of your laptop but do not keep this information with the laptop.

vii. If the laptop is lost or stolen, notify the Police immediately and inform the IT Help/Service Desk as soon as practicable (within hours not days, please).

1.4.2 Virus protection of laptops

i. Viruses are a major threat to DENOSA and laptops are particularly vulnerable if their anti-virus software is not kept up-to-date. The anti-virus software MUST be updated at least monthly. The easiest way of doing this is to simply log on to the DENOSA network for the automatic update process to run. If you cannot log on for some reason, contact the IT Help/Service Desk for advice on obtaining and installing anti-virus updates.

ii. Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive an attachment from that person.

iii. Always ‘virus-scan’ any files downloaded to your computer from any source (Compact Disk/Digital Versatile Disk, USB hard disks and memory sticks, network files, email attachments or files from the Internet). Virus scans normally happen automatically but the IT Help/Service Desk can tell you how to initiate manual scans if you wish to be certain.

iv. Report any security incidents (such as virus infections) promptly to the IT Help/Service Desk in order to minimise the damage.

v. Respond immediately to any virus warning message on your computer, or if you suspect a virus (*e.g*. by unusual file activity), contact the IT Help/Service Desk. Do not forward any files or upload data onto the network if you suspect your Computer might be infected.

vi. Be especially careful to 'virus-scan' your system before you send any files outside of the DENOSA network. This includes EMAIL attachments and CD-ROMs that you create.

1.4.3 Controls against unauthorised access to laptop data

i. Use strong password controls to access your laptop.

ii. You are *personally accountable* for all network and systems access under your user ID, so keep your password secret. Never share it with anyone, not even members of your family, friends or Information Technology staff.

iii. DENOSA laptops are provided for official use by authorised employees. Do not loan your laptop or allow it to be used by others such as family and friends.

iv. Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

1.4.4 Other controls for laptops

i. ***Unauthorised software***

Do not download, install or use unauthorised software programs. Unauthorised software could introduce serious security vulnerabilities into the DENOSA networks as well as affecting the working of your laptop. Software packages that permit the computer to be '*remote controlled*' (*e.g*. *PC anywhere*) and 'hacking tools' (*e.g*. network sniffers and password crackers) are explicitly forbidden on DENOSA equipment unless they have been explicitly pre-authorised by management for legitimate business purposes.

ii. ***Unlicensed software***

Unlicensed software is not permitted on company laptops. Trial licenses (also preauthorised) must be deleted or licensed by the end of the permitted free trial period. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and DENOSA into disrepute by breaking the law.

iii. ***Backups***

All laptop users are responsible for their own backups. Speak to your Business Unit Head for procedures within the Business Unit on backing up your laptop. This is usually done through either a Portable backup device or Online backup onto the DENOSA Cloud. Remember, if the laptop is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the laptop. Off-line backups will save you a lot of heartache and extra work**.**

iv. ***Laws, regulations and policies***

You must comply with relevant laws, regulations and policies applying to the use of computers and information. Software licensing has already been mentioned and privacy laws are another example. Various DENOSA security policies apply to laptops, the data they contain, and network access (including use of the Internet).

v. ***Inappropriate materials***

DENOSA will not tolerate inappropriate material such as pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop and steer clear of dubious websites. IT staff routinely monitor the network and systems for such materials and track use of the Internet: they will report serious/repeated offenders and any illegal materials directly to management, and disciplinary processes will be initiated. If you receive inappropriate material by email or other means, delete it immediately.
If you accidentally browse to an offensive website, click ‘back’ or close the window straight away. If you routinely receive a lot of spam, call IT Help/Service Desk to check your spam settings.

1.5 Health and safety aspects of using laptops

Laptops normally have smaller keyboards, displays and pointing devices that are less comfortable to use than desktop systems, increasing the chance of repetitive strain injury. Balancing the laptop on your knees hardly helps the situation! Limit the amount of time you spend using your laptop. Wherever possible, place the laptop on a conventional desk or table and sit comfortably in an appropriate chair to use it. If you experience symptoms such as wrist pain, eye strain or headaches that you think may be caused by the way you are using the laptop, stop using the device and consult Health and Safety for assistance.

2. Emails Policy

2.1 Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it’s important for users to understand the appropriate use of electronic communications.

2.2 Purpose

The purpose of this email policy is to ensure the proper use of DENOSA email system and make users aware of what DENOSA deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within DENOSA Network.

2.3 Scope

This policy covers appropriate use of any email sent from a DENOSA email address and applies to all employees, vendors, and agents operating on behalf of DENOSA.

2.4 Policy

2.4.1 All use of email must be consistent with DENOSA policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

2.4.2 DENOSA email account should be used primarily for DENOSA business-related purposes; personal communication is permitted on a limited basis, but non-DENOSA related commercial uses are prohibited.

2.4.3 All DENOSA data contained within an email message or an attachment must be secured according to the *Data Protection Standard*.

2.4.4 Email should be retained only if it qualifies as a DENOSA business record. Email is a DENOSA business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

2.4.5 Email that is identified as a DENOSA business record shall be retained according to DENOSA Record Retention Schedule.

2.4.6 The DENOSA email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any DENOSA employee should report the matter to their supervisor immediately.

2.4.7 Users are prohibited from automatically forwarding DENOSA email to a third party email system (noted in 4.8 below). Individual messages which are forwarded by the user must not contain DENOSA confidential or above information.

2.4.8 Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct DENOSA business, to create or memorialize any binding transactions, or to store or retain email on behalf of DENOSA. Such communications and transactions should be conducted through proper channels using DENOSA-approved DENOSA documentation.

2.4.9 Using a reasonable amount of DENOSA resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a DENOSA email account is prohibited.

2.4.10 DENOSA employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.

2.4.11 DENOSA may monitor messages without prior notice. DENOSA is not obliged to monitor email messages.

NB: Policy Compliance

Compliance Measurement

The IT Directorate will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the IT Directorate in advance.

Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action.

2.5 Related Standards, Policies and Processes

2.5.1 Data Protection Standard

Definitions and Terms

None.

3. Ethics Policy

3.1 Overview

DENOSA is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When DENOSA addresses issues proactively and uses correct judgment, it will help set us apart from competitors. DENOSA will not tolerate any wrongdoing or impropriety at any time. DENOSA will take the appropriate measures act quickly in correcting the issue if the ethical code is broken.

3.2 Purpose

The purpose of this policy is to establish a culture of openness, trust and to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behaviour to ensure ethical conduct. Effective ethics is a team effort involving the participation and support of every DENOSA employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

3.3 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at DENOSA, including all personnel affiliated with third parties.

3.4 Policy

3.4.1 Executive Commitment to Ethics

3.4.2 Senior leaders and executives within DENOSA must set a prime example. In any business practice, honesty and integrity must be top priority for executives.

3.4.3 Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.

3.4.4 Executives must disclose any conflict of interests regard their position within DENOSA.

3.4.5 Employee Commitment to Ethics

i. DENOSA employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

ii. Every employee needs to apply effort and intelligence in maintaining ethics value.

iii. Employees must disclose any conflict of interests regard their position within DENOSA.

iv. Employees will help DENOSA to increase customer and vendor satisfaction by providing quality product s and timely response to inquiries.

v. Employees should consider the following questions to themselves when any behavior is questionable:

- Is the behavior legal?
- Does the behavior comply with all appropriate DENOSA policies?
- Does the behavior reflect DENOSA values and culture?

- Could the behavior adversely affect company stakeholders?
- Would you feel personally concerned if the behavior appeared in a news headline?
- Could the behavior adversely affect DENOSA if all employees did it?

3.4.6 Company Awareness

i. Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

ii. DENOSA will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

3.4.7 Maintaining Ethical Practices

i. DENOSA will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.

ii. Employees at DENOSA should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

iii. DENOSA should established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

iv. Employees are required to recertify their compliance to Ethics Policy on an annual basis.

a. Unethical Behavior

i. DENOSA will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

ii. DENOSA will not tolerate harassment or discrimination.

iii. Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.

iv. DENOSA will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

v. DENOSA employees will not use corporate assets or business relationships for personal use or gain.

NB: Policy Compliance

Compliance Measurement

The Corporate Services will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback.

Exceptions
None

Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action.

3.5 Related Standards, Policies and Processes

None.

Definitions and Terms

None.

4. Clean Desk Policy

4.1.1 Overview

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

4.1.2 Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

4.1.3 Scope

This policy applies to all DENOSA employees and affiliates.

4.1.4 Policy

i. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

ii. Computer workstations must be locked when workspace is unoccupied.

iii. Computer workstations must be shut completely down at the end of the work day.

iv. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

v. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

vi. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

vii. Laptops must be either locked with a locking cable or locked away in a drawer.

viii. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
ix. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
x. Upon disposal Restricted and/or Sensitive DENOSA documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
xi. Whiteboards containing Restricted and/or Sensitive information should be erased.
xii. Lock away portable computing devices such as laptops and tablets.
xiii. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive DENOSA documents are not left in printer trays for the wrong person to pick up.

Policy Compliance

Compliance Measurement

The IT Directorate will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the IT Directorate in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

4.1.5 Related Standards, Policies and Processes

None.

Definitions and Terms

None.

5. Server Security Policy

5.1 Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

5.2 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by DENOSA. Effective implementation of this policy will minimize unauthorized access to DENOSA proprietary information and technology.

5.3 Scope

All employees, contractors, consultants, temporary and other workers at DENOSA and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by DENOSA or registered under a DENOSA-owned internal network domain.

5.4 Policy

5.4.1 General Requirements

i. All internal servers deployed at DENOSA must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by ICT. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures

5.4.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the *Audit Policy*.

5.4.2.1 Configuration Requirements

i. Operating System configuration should be in accordance with approved ICT guidelines.

ii. Services and applications that will not be used must be disabled where practical.

iii. Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

iv. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

v. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

vi. Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

vii. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

viii. Servers should be physically located in an access-controlled environment.

ix. Servers are specifically prohibited from operating from uncontrolled cubicle areas.

N:B Monitoring

i. All authorised staff are required to be **signed in and out** of the IT Server Rooms Access Log. These log sheets are retained by the Head of IT. All visitors must also be recorded in the IT Server Rooms Access Log.

ii. Security-related events will be reported to ICT Administrator, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed.

Policy Compliance

Compliance Measurement

The ICT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the ICT team in advance.

Non-Compliance

An employee or elected found to have violated this policy may be subject to disciplinary action.

5.5 Related Standards, Policies and Processes

- Audit Policy
- Equipment Policy

Definitions and Terms

- None

6. Disaster Recovery Plan Policy

6.1 Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives DENOSA a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

6.2 Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by DENOSA that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

6.3 Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

6.4 Policy

6.4.1 Contingency Plans

The following contingency plans must be created:

- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Mass Media Management: Who is in charge of giving information to the mass media?
- Also provide some guidelines on what data is appropriate to be provided.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

Policy Compliance

Compliance Measurement

The IT Directorate will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the IT Directorate in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

6.5 Related Standards, Policies and Processes

None.

Definitions and Terms

- Disaster

7. Password Protection Policy

7.1 Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of DENOSA's resources. All users, including contractors and vendors with access to DENOSA systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

7.2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

7.3 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any DENOSA facility, has access to the DENOSA network, or stores any non-public DENOSA information.

7.4 Policy

7.4.1 Password Creation

7.4.2 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

7.4.3 Users must not use the same password for DENOSA accounts as for other non-DENOSA access (for example, personal ISP account, option trading, benefits, and so on).

7.4.4 Where possible, users must not use the same password for various DENOSA access needs.

7.4.5 User accounts that have system-level privileges granted through group memberships or progra**ms such as S**udo™ must have a unique password from all other accounts held by that user to access system-level privileges.

7.4.6 Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

7.4.7 Password Change

i. All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

ii. All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

iii. Password cracking or guessing may be performed on a periodic or random basis by the **IT Directorate** or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

7.4.8 Password Protection

i. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential DENOSA information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

ii. Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.

iii. Passwords must not be revealed over the phone to anyone.

iv. Do not reveal a password on questionnaires or security forms.

v. Do not hint at the format of a password (for example, "my family name").

vi. Do not share DENOSA passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

vii. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

viii. Do not use the "Remember Password" feature of applications (for example, web browsers).

ix. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

7.4.9 Application Development - Application developers must ensure that their programs contain the following security precautions:

i. Applications must support authentication of individual users, not groups.

ii. Applications must not store passwords in clear text or in any easily reversible form.

iii. Applications must not transmit passwords in clear text over the network.

iv. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

7.4.9 Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

Policy Compliance

Compliance Measurement

The IT Directorate will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the IT Directorate in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

7.5 Related Standards, Policies and Processes

- Password Construction Guidelines

Definitions and Terms

- Simple Network Management Protocol (SNMP)

8 Remote Access Tools Policy

8.1 Overview

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include Team Viewer, LogMeIn, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the DENOSA network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on DENOSA computer systems.

8.2 Purpose

This policy defines the requirements for remote access tools used at DENOSA.

8.3 Scope

This policy applies to all remote access where either end of the communication terminates at a DENOSA computer asset

8.4 Policy

All remote access tools used to communicate between DENOSA assets and other systems must comply with the following policy requirements.

a. Remote Access Tools

DENOSA provides mechanisms to collaborate between internal users, with external partners, and from non-DENOSA systems. The approved software list can be obtained from ITC Department. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

i. All remote access tools or systems that allow communication to DENOSA resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.
ii. The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.
iii. Remote access tools must support the DENOSA application layer proxy rather than direct connections through the perimeter firewall(s).
iv. Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the DENOSA network encryption protocols policy.
v. All DENOSA antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.
vi. All remote access tools must be purchased through the standard DENOSA procurement process, and the information technology group must approve the purchase.

Policy Compliance

Compliance Measurement

The IT Directorate will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the IT Directorate in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

8.5 Related Standards, Policies and Processes

None.

Definitions and Terms

- None

9 Digital Signature Acceptance Policy

9.1 Overview

See Purpose.

9.2 Purpose

The purpose of this policy is to provide guidance on when digital signatures are considered accepted means of validating the identity of a signer in DENOSA electronic DENOSA documents and correspondence, and thus a substitute for traditional “wet” signatures, within the organization. Because communication has become primarily electronic, the goal is to reduce confusion about when a digital signature is trusted.

9.3 Scope

This policy applies to all DENOSA employees and affiliates.

This policy applies to all DENOSA employees, contractors, and other agents conducting DENOSA business with a DENOSA-provided digital key pair. This policy applies only to intra-organization digitally signed DENOSA documents and correspondence and not to electronic materials sent to or received from non-DENOSA affiliated persons or organizations.

9.4 Policy

A digital signature is an acceptable substitute for a wet signature on any intra-organization DENOSA document or correspondence, with the exception of those noted on the site of the Chief Financial Officer (CFO) on the organization’s intranet: <CFO’s Office URL>

The CFO’s office will maintain an organization-wide list of the types of DENOSA documents and correspondence that are not covered by this policy.

Digital signatures must apply to individuals only. Digital signatures for roles, positions, or titles (e.g. the CFO) are not considered valid.

9.4.1 Responsibilities

Digital signature acceptance requires specific action on both the part of the employee signing the DENOSA document or correspondence (hereafter the *signer*), and the employee receiving/reading the DENOSA document or correspondence (hereafter the *recipient*).

9.4.2 Signer Responsibilities

i. Signers must obtain a signing key pair from <DENOSA identity management group>. This key pair will be generated using DENOSA's Public Key Infrastructure (PKI) and the public key will be signed by the DENOSA's Certificate Authority (CA), IT Director.

ii. Signers must sign DENOSA documents and correspondence using software approved by DENOSA IT organization.

iii. Signers must protect their private key and keep it secret.

iv. If a signer believes that the signer's private key was stolen or otherwise compromised, the signer must contact DENOSA Identity Management Group immediately to have the signer's digital key pair revoked.

9.3.3 Recipient Responsibilities

i. Recipients must read DENOSA documents and correspondence using software approved by DENOSA IT department.

ii. Recipients must verify that the signer's public key was signed by the DENOSA's Certificate Authority (CA), IT Director, by viewing the details about the signed key using the software they are using to read the DENOSA document or correspondence.

iii. If the signer's digital signature does not appear valid, the recipient must not trust the source of the DENOSA document or correspondence.

iv. If a recipient believes that a digital signature has been abused, the recipient must report the recipient's concern to DENOSA Identity Management Group.

Policy Compliance

Compliance Measurement

The IT Directorate will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the IT Directorate in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

9.5 Related Standards, Policies and Processes

None.

10 Wireless Communication Policy

10.1 Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

10.2 Purpose

The purpose of this policy is to secure and protect the information assets owned by DENOSA. DENOSA provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. DENOSA grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to DENOSA network. Only **those** wireless infrastructure devices that meet the standards **specified in** this policy or are granted an exception by the Information Security Department are approved for connectivity to a DENOSA network.

10.3 Scope

All employees, contractors, consultants, temporary and other workers at DENOSA, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of DENOSA must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a DENOSA network or reside on a DENOSA site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

10.4 Policy

General Requirements

All wireless infrastructure devices that reside at a DENOSA site and connect to a DENOSA network, or provide access to information classified as DENOSA Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use DENOSA approved authentication protocols and infrastructure.
- Use DENOSA approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

a. Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to DENOSA Confidential or above, must adhere to section 4.1 above. Lab and isolated wireless devices that do not provide general network connectivity to the DENOSA network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the Lab Security Policy.

- Not interfere with wireless access deployments maintained by other support organizations.

b. Home Wireless Device Requirements

   i. Wireless infrastructure devices that provide direct access to the DENOSA corporate network, must conform to the Home Wireless Device Requirements as detailed in the *Wireless Communication Standard*.

   ii. Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the DENOSA corporate network. Access to the DENOSA corporate network through this device must use standard remote access authentication.

Policy Compliance

a. Compliance Measurement

The IT Directorate will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

b. Exceptions

Any exception to the policy must be approved by the IT Directorate in advance.

c. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

10.5 Related Standards, Policies and Processes

- Lab Security Policy
- Wireless Communication Standard

11 Technology Equipment Disposal Policy

11.1 Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of DENOSA data, some of which is considered sensitive. In order to protect our constituent’s data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

11.2 Purpose

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by DENOSA.

11.3 Scope

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within DENOSA including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials.

All DENOSA employees and affiliates must comply with this policy.

11.4 Policy

a. **Technology Equipment Disposal**

i. When Technology assets have reached the end of their useful life they should be sent to the IT Directorate office for proper disposal.

ii. The IT Directorate will securely erase all storage mediums in accordance with current industry best practices.

iii. All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defense standards.

iv. No computer or technology equipment may be sold to any individual other than through the processes identified in this policy (Section 4.b below).

v. No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around DENOSA. These can be used to dispose of equipment. The IT Directorate will properly remove all data prior to final disposal.

vi. All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

vii. Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

viii. The IT Directorate will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.

ix. Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

b. **Employee Purchase of Disposed Equipment**

i. Equipment which is working, but reached the end of its useful life to DENOSA, will be made available for purchase by employees.

ii. A lottery system will be used to determine who has the opportunity to purchase available equipment.

iii. All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or “reserve” a system. This ensures that all employees have an equal chance of obtaining equipment.

iv. Finance and Information Technology will determine an appropriate cost for each item.

v. All purchases are final. No warranty or support will be provided with any equipment sold.

vi. Any equipment not in working order or remaining from the lottery process will be donated or disposed of according to current environmental guidelines. Information

vii. Technology has contracted with several organizations to donate or properly dispose of outdated technology assets.

viii. Prior to leaving DENOSA premises, all equipment must be removed from the Information Technology inventory system.

Policy Compliance

Compliance Measurement

The IT Directorate will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the IT Directorate in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

11.5 Related Standards, Policies and Processes

None.

Definitions and Terms

None.

12 Web Application Security Policy.

12.1 Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities by remediated prior to production deployment.

12.2 Purpose

The purpose of this policy is to define web application security assessments within DENOSA. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of DENOSA services available both internally and externally as well as satisfy compliance with any relevant policies in place.

12.3 Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at DENOSA.

All web application security assessments will be performed by delegated security personnel either employed or contracted by DENOSA. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of DENOSA is strictly prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be DENOSA document prior to the start of the assessment.

12.4 Policy

a. Web applications are subject to security assessments based on the following criteria:
    i. New or Major Application Release – will be subject to a full assessment prior to approval of the change control DENOSA documentation and/or release into the live environment.
    ii. Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.
    iii. Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
    iv. Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
    v. Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

b. All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.
    i. High – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
    ii. Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment

based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.

iii. Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

c. The following security assessment levels shall be established by the IT Directorate organization or other designated organization that will be performing the assessments.

i. Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.

ii. Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

iii. Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

d. The current approved web application security assessment tools in use which will be used for testing are:

- <TBE>
- <TBE>
- <...>

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

Policy Compliance

a. Compliance Measurement

The IT Directorate will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

b. Exceptions

Any exception to the policy must be approved by the IT Directorate in advance.

c. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

12.5 Related Standards, Policies and Processes

OWASP Top Ten Project:
http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP Testing Guide: http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

OWASP Risk Rating Methodology:
http://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Definitions and Terms

None.

13. Acceptable Use Policy

13.1 Overview

IT Directorate’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to DENOSA’s established culture of openness, trust and integrity. IT Directorate is committed to protecting DENOSA's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of DENOSA. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every DENOSA employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

13.2 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at DENOSA. These rules are in place to protect the employee and DENOSA.

Inappropriate use exposes DENOSA to risks including virus attacks, compromise of network systems and services, and legal issues.

13.3 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct DENOSA business or interacts with internal networks and business systems, whether owned or leased by DENOSA, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at DENOSA and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with DENOSA policies and standards, and local laws and regulation. Exceptions to this policy are DENOSA documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at DENOSA, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by DENOSA.

13.4 Policy

13.4.1 General Use and Ownership

13.4.1.1 DENOSA proprietary information stored on electronic and computing devices whether owned or leased by DENOSA, the employee or a third party, remains the sole property of DENOSA. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

13.4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of DENOSA proprietary information.

13.4.1.3 You may access, use or share DENOSA proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

13.4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

13.4.1.5 For security and network maintenance purposes, authorized individuals within DENOSA may monitor equipment, systems and network traffic at any time, per IT Directorate's *Audit Policy*.

13.4.1.6 DENOSA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

13.4.2 Security and Proprietary Information

13.4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.

13.4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

13.4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

13.4.2.4 Postings by employees from a DENOSA email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of DENOSA, unless posting is in the course of business duties.

13.4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

13.4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of DENOSA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing DENOSA-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

13.4.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by DENOSA.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which DENOSA or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting DENOSA business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a DENOSA computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any DENOSA account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to IT Directorate is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Introducing honeypots, honeynets, or similar technology on the DENOSA network.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, DENOSA employees to parties outside DENOSA.

13.4.5 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

i. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

ii. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

iii. Unauthorized use, or forging, of email header information.

iv. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

v. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

vi. Use of unsolicited email originating from within DENOSA's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by DENOSA or connected via DENOSA's network.

vii. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

viii. Blogging by employees, whether using DENOSA’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of DENOSA’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate DENOSA’s policy, is not detrimental to DENOSA’s best interests, and does not interfere with an employee's regular work duties. Blogging from DENOSA’s systems is also subject to monitoring.

ix. DENOSA’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any DENOSA confidential or proprietary information, trade secrets or any other material covered by DENOSA’s Confidential Information policy when engaged in blogging.

x. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of DENOSA and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by DENOSA’s *Non-Discrimination and Anti-Harassment* policy.

xi. Employees may also not attribute personal statements, opinions or beliefs to DENOSA when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of DENOSA. Employees assume any and all risk associated with blogging.

xii. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, DENOSA’s trademarks, logos and any other DENOSA intellectual property may also not be used in connection with any blogging activity

Policy Compliance

Compliance Measurement

The IT Directorate team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the IT Directorate team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

13.5 Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

Revision History

Date of Change	**Responsible**	**Summary of Change**
Dec 2021	Policy Team/NEC/NOB	Updated and converted to new format

14 Forms and Declaration

Hardware and Software Use

1. In terms of the Copyright Act (Act No. 98) of 1978, as amended, computer programmes are now specifically protected and may only be used by persons who are in lawful possession of legitimate programs. DENOSA strongly adheres to such a policy and hereby informs the DENOSA staff member of same

2. During the course of his/her employment or engagement at DENOSA, the DENOSA staff member may be provided with a notebook, desktop, software and other hardware according to his/her identifiable need commensurate with the activities that DENOSA deems necessary for the DENOSA staff member to fulfil during the tenure of his/her employment or engagement and available budget. DENOSA reserves the sole right to withdraw and thus terminate the right of use of the notebook, desktop, software and other hardware, at any time and upon any grounds that it, in its exclusive opinion, deems appropriate.

3. The DENOSA staff member undertakes, and acknowledges, that such an undertaking is of the utmost importance to DENOSA and should he/she breach such an undertaking same shall be construed as a material breach of this clause, that upon his/her termination of employment or engagement with DENOSA for whatever reason and howsoever arising, he/she shall forthwith return the notebook, desktop, software and other hardware that he/she received upon his/her commencement of employment or engagement with DENOSA, to his/her superior or that individual’s chosen representative or substitute. The DENOSA staff member acknowledges and accepts unequivocally that the notebook, desktop software and other hardware supplied by DENOSA to him/her is, and will always remain, the sole and exclusive property of DENOSA. The DENOSA staff member understands that by being provided with the notebook, desktop, software and other hardware, DENOSA is not in any manner or form transferring its sole proprietary interests in the notebook, desktop software or other hardware to the DENOSA staff member.

4. Upon the return of all the items listed in clause 3 above, a full and complete investigation of the returned items shall be undertaken by DENOSA. The DENOSA staff member is required to return the notebook, desktop, software and other hardware in the same condition in which he/she received same upon commencement of employment or engagement with DENOSA.

5. The DENOSA staff member shall not be permitted to, without the express and prior written authority of the DENOSA staff member’s superior, in any way, delete, erase, transfer, substitute, change, disassemble, transform or in any way tamper with the notebook, desktop, software and other hardware.

6. The notebook, desktop, software and other hardware, shall be used exclusively, and without exception, during the course and scope of the DENOSA staff member's employment or engagement with DENOSA. Under no circumstances shall the DENOSA staff member be permitted to utilise the notebook, desktop, software or other hardware for purposes other than those associated with his/her assigned duties and responsibilities on behalf of DENOSA, save for reasonable personal
business which does not interfere with his/her normal assigned duties and responsibilities.

7. While DENOSA maintains liability insurance to repair or replace the notebook, desktop or other hardware if it is lost, stolen or damaged, it will be the DENOSA staff member's responsibility to perform due diligence to prevent damage to or loss/theft of the aforesaid items. The DENOSA staff member may be responsible for costs to repair or replace the mentioned items if the damage or loss is due to negligence or intentional misconduct or omission. The burden of proof resides with the DENOSA staff member and the DENOSA staff member agrees to assume full responsibility to show proof of due care.

8. The DENOSA staff member shall be responsible for maintaining appropriate backups.

9. The playing of computer games using the notebook, desktop, software and other hardware provided by DENOSA to the DENOSA staff member, is banned. The DENOSA staff member is also prohibited from utilizing the notebook, desktop, software or other hardware in installing, using, viewing and accessing pornographic material, social websites, illegal software, software that has been registered with another company, or software or content DENOSA deems is generally inappropriate as notified by DENOSA to the DENOSA staff member from time to time.

10. In the event that the staff member fails, either wilfully or through negligence on his/her part, to return the notebook, desktop, software or other hardware on the agreed return date as specified in the Technology Checkout Form to which these terms are annexed, or upon an alternative date elected by DENOSA at its sole discretion and which date is brought to the attention of the staff member, the staff member consents to have the full value of the notebook, desktop, software or other hardware deducted from his/her salary, remuneration, or payment with the balance thereof, if any, to be paid over to him or her. In the event that the staff member's salary, remuneration, or payment is less than the value of the non-returned notebook, desktop, software or other hardware, then DENOSA shall reserve its rights in terms of clause 7 above.

11. DENOSA staff members who are in breach of these terms will be disciplined according to DENOSA's internal disciplinary proceedings and/or be subject to legal proceedings, both civil and criminal.

I, ____________________________________, acknowledge that I have read and understood the above terms of this policy.

Signed By _______________________ Date ______________________

2. DENOSA Staff End-User Declaration (Annexure A)

INFORMATION TECHNOLOGY

USER DECLARATION AGREEMENT

I acknowledge that access to information technology resources and services is granted to me for performing DENOSA work and responsibilities.

I have read and agree to abide by the Departmental IT policies and procedures that govern my use of these services:

I will refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, disk space, printer paper, email and internet services or other information technology resources.

I will report to the DENOSA management any observations of attempted security violations or illegal activities.

I will report to the DENOSA management if I receive or obtain information to which I am not entitled.

I further acknowledge that any unacceptable use by me in accordance to any IT Policy will constitute an act or acts of misconduct that may during an investigating process result in the suspension of my specific and or network access privileges without notice and or my knowledge; and or result in disciplinary action being instituted against me which may result in the termination of my access privileges.

By signing this agreement, I certify that I understand and accept responsibility for adhering to the policies, procedures, and additional DENOSA terms and conditions listed above.

Employee Name (Print): ________________________________

Employee Number: ________________________________

Employee Signature: ________________________________

Date: _______________________________