CONTENTS

IT PROCEDURES

1. ADMINISTRATIVE RIGHTS PROCEDURE

Administrative rights give users the ability to change system configurations and download software, installing unauthorized software, potentially opening up the network to vulnerability. Holding administrative rights over a desktop, laptop or other end-user device shouldn't be seen as a "right" – it is a privilege that must be protected from abuse.

1.1. Purpose

This Administrator Rights Procedure sets out Grindrod Shipping's procedure on the assignment and use of administrator rights (also sometimes referred to as "superuser" privileges).

The granting of administrative rights to an employee of Grindrod Shipping over an individual desktop, laptop, or other end-user device is a privilege only awarded to individuals who require this level of access and control in order to do their jobs effectively. The goal of this procedure is to describe the circumstances under which administrative rights can be granted as well as the terms and conditions upon which this privilege will be granted.

1.2. Scope

This procedure applies to all users of all computer equipment owned, supplied or maintained by Grindrod Shipping including servers, desktop computers, laptops and portable devices. This excludes mobile and smart phone devices.

1.3. Procedure

Running a computer system with administrator rights represents a significant risk to the confidentiality, integrity and availability of Grindrod Shipping's information assets. It is also unnecessary for the overwhelming majority of Grindrod Shipping staff.

It is Grindrod Shipping procedure not to assign administrator rights to members of staff except where necessary. Where such privileges are granted, it is procedure that these privileges will only be used for system administration purposes (updating software, for example) and will not be used for "day to day" activities (web browsing or email processing, for example).

The granting of administrative rights allows the individual to change the configuration settings of a given machine and install software on that machine. As a result, these rights can expose the Grindrod Shipping network to malware and other security exploits. In addition, incorrect configuration of machines can lead to performance problems, potentially resulting in machine downtime, lost productivity, and higher support costs.

Given the serious consequences of mishandling or abuse of administrative rights, these rights will only be granted under the condition that they are essential for the performance of the grantee's job. Such conditions could include the following:

a. The ability to download and install specific types of software or configure system settings is mandated in the individual's job description.

b. Sufficient levels of IT support do not exist due to time-of-day, geographical or expertise constraints.

Typically, the only individuals at Grindrod Shipping who are granted administrative rights include:

Function	Requirement for Administrative Rights
Desktop Support Technician	Set up desktops and laptops for end users. Provide desk-side and remote support to desktop and laptop users.
System Administrators	Set up of servers for the businesses. Provide application and server support to desktop and laptop users.
Vendors and Support	Setup and Support of systems under IT supervision

Note: Members of the IT Department are not automatically granted administrative rights based on their membership in the IT Department alone.

If you do not perform one of the functions described in the table above, then you will need to apply and gain approval for administrative rights if you believe it is required by your job. To apply for administrative rights, please use the Administrative Rights Application Form located at the end of this procedure document. The designated authorities of the IT Department reserve the right to deny the application if it does not represent a clear business need or if the applicant has a documented history of security procedure violation.

1.4. Disclaimer

If you have been granted administrative rights, you must adhere to the following disclaimer:

1.4.1. You will comply with all existing technology appropriate use procedures of Grindrod Shipping.

1.4.2. You will not make changes to any desktop, laptop or other end-user device not assigned to you personally.

1.4.3. IT support employees who are mandated in their job descriptions to make changes to desktops, laptops, or other end-user devices will only make such changes as are authorized and assigned to them personally.

1.4.4. You will not install any unauthorized or non-standard software at any time.

1.4.5. You will take all reasonable steps to ensure that the desktop, laptop or other end-user device over which you have administrative rights is secured from malware or intrusion.

1.4.6. You will have sole responsibility for backing up any data stored to the desktop, laptop or other end-user device over which you have administrative rights.

1.4.7. The IT Department will provide complete support and troubleshooting for the standard base image issued with the machine. Support for non-standard software installed by an employee exercising administrative rights is limited to the following:

NOTE: Grindrod Shipping IT will NOT support unapproved software installations.

1.5. Non-Compliance Penalties

Penalties for violation of this procedure will vary depending on the nature and severity of the violation. Penalties include:

- Disciplinary action, including, but not limited to, reprimand, suspension and/or termination of employment.

2. ANTI-VIRUS

2.1. Purpose

This procedure is designed to protect the organisational resources against intrusion by viruses and other malware.

This is an internal IT procedure which defines the anti-virus application on every computer including how often a virus scan is done, how often updates are done, and what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked at the mail filter and what anti-virus program will be run on the mail server. It also specifies the anti-spam firewall used to provide additional protection to the mail server. It may also specify how files can enter the trusted network and how these files will be checked for hostile or unwanted content. Files sent to Grindrod Shipping from outside the trusted network are scanned for viruses by specific Anti-virus programs.

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via multiple media, including e-mail or instant messaging attachments, downloadable Internet files, memory sticks, portable drives and CDs or DVD's. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to Grindrod Shipping in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of Grindrod Shipping is to provide a computing network that is virus-free. The purpose of this procedure is to provide instructions on measures that must be taken by Grindrod Shipping employees to help achieve effective virus detection and prevention.

2.2. Scope

This procedure applies to all Grindrod Shipping owned computers that are connected to the Grindrod Shipping network via a standard network connection, wireless connection, modem connection, or virtual private network connection. The definition of computers includes desktop workstations, laptop computers, and servers.

2.3. General Procedure

2.3.1. Currently, Grindrod Shipping has a subscription for the ESET Anti-Virus. Licensed copies of ESET Anti-Virus will be installed by IT Services. The most current available version of the anti-virus software package will be taken as the default standard.

2.3.2. All Grindrod Shipping owned computers attached to the Grindrod Shipping network must have standard, supported anti-virus software installed. This software must be active and have its virus definition files kept up to date.

2.3.3. Any activities with the intention to create and/or distribute malicious programs onto the Grindrod Shipping network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

2.3.4. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the IT. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

2.3.5. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT department.

2.3.6. Any virus-infected computer will be removed from the network until it is verified as virus-free.

2.4. Rules for Virus Prevention

2.4.1. Always run the standard anti-virus software provided by Grindrod Shipping.

2.4.2. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

2.4.3. Never open any files or macros attached to an e-mail from a known source (even a co-worker) if you were not expecting a specific attachment from that source.

2.4.4. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

Do not depend on your anti-virus software on each computer to prevent these viruses. Viruses have a period of time when they spread unrecognized by anti-virus software. Blocking these file attachments will prevent many trouble calls.

The Grindrod Shipping solution will depend on the Grindrod Shipping network and the software that is being used to block the file attachments. In some cases, Grindrod Shipping IT could rename the file to another type and instruct the recipient to rename it back to the original name before using it. This will not work in all cases since some file blocking software senses the actual file type regardless of its named file extension.

When an email breaks the rules, and contains an illegal file attachment the following will be done:

- The email and all attachments will be blocked entirely and a notification sent to both sender and recipient stating that the mail has been blocked and why. If the attempt was a legitimate one, they could contact the sender and tell them what to do to get the attachment sent. There is no ideal procedure here and the Grindrod Shipping system administrators must choose the best method depending on the situation being experienced.

2.4.5. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

2.4.6. Avoid direct portable drive (e.g. memory stick) sharing with read/write access. Always scan a portable drive for viruses before using it.

2.4.7. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Recycle Bin folder.

2.4.8. Back up critical data and systems configurations on a regular basis and store backups in a safe place.

2.4.9. Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

2.5. Anti-SPAM Procedure

SPAM is the IT name given to what us generally known as “junk mail”. Whist not necessarily destructive, SPAM has a debilitating effect on network and mail resources, and ultimately represents a waste of resources.

Grindrod Shipping subscribes to an Anti-SPAM service which maintains a filter system, updated hourly, on all known SPAM domains. This filter system, on Grindrod Shipping’s external network gateway, identifies and deletes all known SPAM mail.

Whilst effective, the Anti-SPAM filter only removes approximately 95% of all SPAM. The balance of SPAM mail will be delivered to user devices.

The following rules should be applied to SPAM messages arriving in a user mailbox:

- Never reply to a SPAM message or open attachments
- Delete SPAM messages as soon as they arrive in the mail box (a message from an unknown source with an unbelievable subject line can be treated as rubbish).

2.6. IT Department Responsibilities

The following activities are the responsibility the IT department:

a. The IT department is responsible for maintaining and updating this Anti-Virus application.

b. The IT department will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use.

c. The IT department will apply any updates to the services it provides that are required to defend against threats from viruses.

d. The IT department will install anti-virus software on all Grindrod Shipping owned and installed desktop workstations, laptops, and servers on the network.

e. The IT department will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

f. The IT department will perform anti-virus sweeps on demand.

g. On-access scan is permanently enabled to scan any file that is opened on the user device. This procedure forbids the turning off of the on-access scan on any device.

h. The IT department will attempt to notify users of Grindrod Shipping systems of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

2.7. Department and Individual Responsibilities

The following activities are the responsibility of all departments and employees:

a. Departments must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this procedure.

b. Departments that allow employees to use personally-owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this procedure.

c. All employees are responsible for taking reasonable measures to protect against virus infection.

d. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the network without the express written consent of the IT department.

2.8. Enforcement

Any employee who is found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

3. ASSET DISPOSAL

3.1. Overview

Asset retirement can be an extremely risky process associated with potentially devastating fines and lawsuits.

The purpose of this Procedure is to establish and define standards, procedures and restrictions for the disposal of non-leased IT equipment in a legal, cost-effective manner. Grindrod Shipping's surplus or obsolete IT assets and resources (i.e. desktop computers, servers, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and Grindrod Shipping's upgrade guidelines. Therefore, all disposal procedures for retired IT assets must adhere to company-approved methods.

3.2. Responsibility

IT equipment disposal is managed and coordinated by the vessel under the guidance of IT. In addition, this department is responsible for backing up and then wiping clean company data on all IT assets slated for disposal.

3.3. Practices

Acceptable methods for the disposal of IT assets are as follows:

a. Discarded to an approved service provider capable of processing e-waste. The Garbage Record book is to be filled in accordingly.

It is imperative that any disposals performed by Grindrod Shipping are done appropriately, responsibly and ethically, as well as with company resource planning in mind. The following rules must therefore be observed:

3.3.1. Obsolete IT Assets: Obsolete refers to any and all computer or computer-related equipment written off and / or equipment that no longer meets requisite functionality. Identifying and classifying IT assets as obsolete is the sole province of the IT department.

3.3.2. Reassignment of Retired Assets: Reassignment of computer hardware to a less-critical role is made at the sole discretion of IT department

3.3.3. Donations: IT assets with a nominal net residual value that are not assigned for reuse, discarding or sale to employees or external buyers, may be donated to a school, charity or other non-profit organisation (i.e. a distributor of free machines to developing nations).

4. DESKTOP AND USER MOVE / ADD / REMOVAL / CHANGE

4.1. Procedure

All move, removal, add, or change requests must be approved by Management. This procedure is to help control the move/add/removal/change process and keep support costs low. Contact IT Helpdesk if you wish to:

a. Move a desktop system or peripheral to another physical or network location;

b. Add/remove software or hardware to/from an existing desktop system;

c. Add/disable an employee account; add/remove a service to/from an existing employee account;

d. Add/remove a new employee desktop system;

e. Change an employee's name or other personally identifiable information in the system;

4.2. Purpose

This procedure provides guidelines for end users to request a move, add, or change to their desktop computing environments and the process for adding, changing or removing an employee account. The goal of this procedure is:

a. To mitigate the risk associated with unauthorised changes;

b. To minimise disruption to the business, IT and end users;

4.3. Sample Outage Notification E-mail Message:

From: Grindrod Shipping Shipping IT Call Centre / IMMARSAT

Sent: January 27, 2011 10:37 AM

To: [Employee name/ Ships Name]

Subject: Scheduled Outage Notification

Scheduled Outage:

On February 7, 2011 your [e.g. telephone service] will be taken offline for [e.g. maintenance] from 17:00 to 18:00.

During the outage, you will not be able to (e.g.) make or receive calls, and voicemail will be disabled.

If you have any questions or concerns related to this outage, please contact the IT

Thank you for your cooperation,

4.4. Management

Ownership of this procedure falls to IT Manager

4.5. Review

Management is responsible for keeping this procedure current. This procedure will be reviewed annually or as circumstances arise.

5. DOWNTIME

5.1. Purpose

Grindrod Shipping is committed to ensuring reliable information technology services. In order to meet this objective, Grindrod Shipping systems may need to be taken offline to maintain or improve system performance, safeguard data or to respond to emergency situations.

5.2. Planned Downtime

From time to time, it will be necessary to make systems unavailable for the purpose of performing upgrades, maintenance, or housekeeping tasks. The goal of these tasks is to ensure maximum system performance and prevent future system failures. The following activities fall within the definition of Planned Downtime:

a. Application of patches to operating systems and other applications in order to fix vulnerabilities and bugs, add functionality or improve performance

b. Disk defragmentation, disk clean-up and other general disk maintenance operations

c. Required upgrades to system physical memory or storage capacity

d. Installation or upgrade of applications or services, including networks and other communication systems

e. System performance tuning

f. Offline backup of database applications

g. If a parent system is going to be down, the dependent system will have to be brought down at the same time.

Every effort will be made to perform the procedure during off-hours in order to minimise the impact on those who use the affected systems or services. On occasion, it may be necessary to have Planned Downtime during regular business hours, but this is an exception and only when an emergency occurs.

If this is the case, then this Planned Downtime will be communicated to all users of affected resources using the Notification of Downtime mechanism described below.

5.3. Emergency Downtime

Unexpected circumstances may arise where systems or services will be interrupted without prior notice. Every effort will be made to avoid such circumstances. However, incidences may arise involving a compromise of system security, the potential for damage to equipment or data or emergency repairs. If the affected system(s) cannot be brought back online within five (5) to ten (10) minutes, affected users will be contacted via the Notification of Downtime mechanism described below.

5.4. Notification of Downtime

Users will be notified of downtime according to the following procedure:

a. The IT management representative responsible for the system in question is responsible for notifying all identified users of Planned Downtime, as well as any unplanned interruptions to system availability as they occur

b. If general maintenance procedures will cause Planned Downtime during regular business hours, and the procedure will last less than two (2) hours, then the system administrator must notify system users at least two (2) hours prior to the Planned Downtime

c. If Planned Downtime beyond general maintenance is scheduled that will last longer than two (2) hours, then the system administrator must give one (1) business day notice for every hour of anticipated system unavailability. This step must be taken regardless of whether the downtime is scheduled to take place during off hours or regular business hours

d. In the event of Emergency Downtime, the system administrator will use his/her discretion in notifying end users of the situation. In emergency circumstances where time is of the essence, it may not be possible for the system administrator to engage in normal downtime notification activities. When emergency measures are completed, or if thirty (30) minutes has elapsed with no resolution, then the system administrator will contact all affected users or their elected representative with information on system status and/or information on additional expected downtime.

All downtime announcements will provide the following information:

a. Systems and services that are affected, as well as suggested alternatives to them (if any)

b. Start and end times of the Planned Downtime period, or estimated time to recovery, in the event of Emergency Downtime

c. The reasons why the downtime is taking place

d. Any ongoing problems that are anticipated as a result of the downtime event and the contact details for the responsible person within IT that should be contacted in the event of problems occurring after the downtime period is complete.

6. E-MAIL ACCEPTABLE USE

6.1. Overview

Email is a critical mechanism for business communications at Grindrod Shipping.

An email record can be interpreted and used in court as a legal document, including a business transaction.
This Procedure outlines appropriate and inappropriate use of Grindrod Shipping's email systems and services in order to minimise disruptions to services and activities, as well as comply with applicable policies and laws.

6.2. Scope

This Procedure applies to all email systems and services owned by Grindrod Shipping, all email account users at Grindrod Shipping (both temporary and permanent) and all company email records.

6.3. General Expectations of End Users

The enterprise often delivers official communications via email. As a result, employees of Grindrod Shipping with email accounts are expected to check their email in a consistent and timely manner so that they are aware of important company announcements and updates, as well as for fulfilling business and role-oriented tasks.

Email users are responsible for mailbox management, including organisation and housekeeping. If a user subscribes to a mailing list, he or she must be aware of how to unsubscribe from the list and is responsible for doing so in the event that their current email address changes.

Email users are expected to remember that email sent from Grindrod Shipping email accounts reflects on Grindrod Shipping and they have a duty to comply with normal standards of professional and personal courtesy and conduct.

6.4. Appropriate Use

Individuals at Grindrod Shipping are encouraged to use email to further the goals and objectives of Grindrod Shipping. The types of activities that are encouraged include:

a. Communicating with fellow employees, business partners of Grindrod Shipping and clients within the context of an individual's assigned responsibilities
b. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.

6.5. Inappropriate Use

Grindrod Shipping's email systems and services are not to be used for purposes that could be reasonably expected to strain storage or bandwidth (e.g. emailing large attachments instead of pointing to a location on a shared drive). Individual email use will not interfere with others' use of Grindrod Shipping's email system and services. Email use at Grindrod Shipping will comply with all applicable laws, all Grindrod Shipping procedures and all Grindrod Shipping contracts.

The following activities are deemed inappropriate uses of Grindrod Shipping email systems and services, and are strictly prohibited:

a. Use of email for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, racism, religion, pornography, soliciting for illegal pyramid schemes and computer tampering (e.g. spreading of computer viruses)

b. Forwarding chain mail messages

c. Use of email in any way that violates Grindrod Shipping's policies, rules or administrative orders, including, but not limited to, the Grindrod Shipping Employees Code of Conduct

d. Viewing, copying, altering or deletion of email accounts or files belonging to Grindrod Shipping or another individual without authorised permission

e. Sending of unreasonably large email attachments. The total allowed size of an individual email message sent (including attachment) is 10MB, unless other arrangements have been made

f. Opening email attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution

g. Sharing email account passwords with another person or attempting to obtain another person's email account password. Email accounts are only to be used by the registered user

h. Excessive personal use of Grindrod Shipping email resources. Grindrod Shipping allows limited personal use for communication with family, friends and public service so long as it does not interfere with staff productivity, pre-empt any business activity or consume more than a trivial amount of resources. Grindrod Shipping prohibits personal use of its email systems and services for unsolicited mass mailings, non-Grindrod Shipping commercial activity, political and religious campaigning, dissemination of chain letters and pornographic materials and use by non-employees.

i. Using the system for any activity that may harm or defamation of the brand of Grindrod Shipping.

j. To conduct private business from a Grindrod Shipping domain address

6.6. Monitoring and Confidentiality

The email systems and services used at Grindrod Shipping are owned by the company and are therefore its property. Grindrod Shipping has the right to monitor any and all email traffic passing through its email system. This monitoring may include, but is not limited to, inadvertent reading by authorised IT staff during the normal course of managing the email system, review by the legal team during the email discovery phase of litigation, observation by management in cases of suspected abuse or to monitor employee efficiency.

In addition, archival and backup copies of email messages exist, despite end-user deletion, in compliance with Grindrod Shipping's records retention procedure and the Applicable National regulations. The goals of these backup and archiving procedures are to ensure system reliability, prevent business data loss, meet regulatory and litigation needs and to provide business intelligence.

Backup copies exist primarily to restore service in case of failure. Archival copies are designed for quick and accurate access by company delegates for a variety of management and legal needs. Both backups and archives are governed by the company's document retention policies. These policies indicate that email must be kept for up to seven (7) years. Email retention procedure is managed in the same way as any other record retention within Grindrod Shipping.

If Grindrod Shipping discovers or has good reason to suspect activities that do not comply with applicable laws or this procedure, email records may be retrieved and used to document the activity in accordance with due process. All reasonable efforts will be made to notify an employee if his or her email records are to be reviewed, however this is not a prerequisite and the company retains the right to scan all emails that make use of the company facilities.

Use extreme caution when communicating confidential or sensitive information via email. Keep in mind that all email messages sent outside of Grindrod Shipping become the property of the receiver. A good rule is to not communicate anything that you wouldn't feel comfortable being made public. Demonstrate particular care when using the "Reply to All" command during email correspondence to ensure the resulting message is not delivered to unintended recipients.

6.7. Reporting Misuse

Any allegations of misuse should be promptly reported to the Grindrod Shipping IT Services Manager. Do not forward, delete or reply to an offensive email.

7. INTELLECTUAL PROPERTY

7.1. Rationale

Grindrod Shipping has a legal right and duty to:

a. Identify its intellectual property (IP) assets;

b. Own IP assets created by its employees or on its behalf;

c. Enhance the value of its IP assets; and

d. Take the necessary actions to protect its IP assets from unauthorised use and disclosure.

7.2. Purpose

The purpose of this Procedure is to:

a. Properly identify and maintain an updated list of Grindrod Shipping's IP assets;

b. Ensure Grindrod Shipping owns its IP assets;

c. Enhance the value of Grindrod Shipping's IP assets;

d. Protect Grindrod Shipping's IP assets; and

e. Prevent the unauthorised use of Grindrod Shipping's IP assets.

7.3. Ownership of IP

7.3.1. General IP ownership rules

7.3.1.1. As a general rule, and unless stated otherwise in this Procedure, Grindrod Shipping shall own IP that is:

a. Created by or originated from an employee, in whole or in part, as a direct result of his/her employment with Grindrod Shipping; or

b. Created or originated by a Content Provider, in whole or in part, in terms of a written agreement whereby IP is created for Grindrod Shipping in return for a fee or payment or other form of compensation.

7.3.1.2. No person shall appoint or procure the services of a Content Provider unless such appointment of procurement is governed by a written agreement that addresses, at the very least, the following items:

a. Transfer of ownership of IP created by the Service Provider to Grindrod Shipping

b. Moral rights waiver

c. Warranties by the Content Provider that IP created by it does not violate third-party copyright.

7.3.2. Exceptions to the general IP ownership rule.

7.3.2.1. IP will be owned by an employee or Content Provider if;

a. Its creation did not involve the use of any of Grindrod Shipping's resources; and

b. It was not created, in whole or in part, during regular office hours; and

c. It was not created as a result of the employee's employment responsibilities or a Content Provider's responsibilities in terms of a written agreement entered into between such Content Provider and Grindrod Shipping.

7.4. Situations Where Grindrod Shipping Wishes to Use External IP (e.g. Software)

7.4.1. If Grindrod Shipping wishes to use External IP in any way whatsoever, it shall do so through a licence agreement concluded between Grindrod Shipping and the owner of such External IP. Such agreement shall;

a. Be in writing;

b. Clearly state the rights in the IP that Grindrod Shipping may exploit

c. Clearly state whether electronic use of these rights is permitted or not

d. State the term during which such rights may be exploited

e. State the territory or territories in which such rights may be exploited

f. Include a warranty from the external party that:

- He / she / it has the full right or licence to grant such rights to Grindrod Shipping; and
- Exploitation of such rights by Grindrod Shipping shall not infringe any third party's IP rights.

7.4.2. This clause also applies to all software-related licences.

7.5. Situations Where Other Businesses or Individuals Wish to Use IP of Grindrod Shipping (e.g. Brands, Website Content and the Like)

7.5.1. If Grindrod Shipping wants to license an external party to exploit IP of Grindrod Shipping, it shall do so through a licence agreement concluded between Grindrod Shipping and such external party. Such agreement shall:

a. Be in writing;

b. Clearly state the IP rights the external party may exploit;

c. Clearly state whether electronic use of such IP rights is permitted or not;

d. State the term during which such rights may be exploited; and

e. State the territory or territories within which such rights may be exploited.

7.6. Non-Disclosure Agreements

7.6.1. All non-disclosure agreements entered into by Grindrod Shipping shall be signed by the responsible person as appointed by Grindrod Shipping and no other person.

7.6.2. As far as reasonably possible a standard Grindrod Shipping non-disclosure agreement shall be used.

7.7. Trademarks

7.7.1. Grindrod Shipping shall be responsible for the registration and maintenance of all Grindrod Shipping's trademarks.

7.7.2. All Grindrod Shipping company names, brand names and products/services shall be registered as Grindrod Shipping trademarks.

7.8. Domain Names

7.8.1. Grindrod Shipping IT shall be responsible for the registration and maintenance of all Grindrod Shipping's domain names.

7.8.2. All Grindrod Shipping company names, brand names, trademarks and products/services shall be registered as Grindrod Shipping trademarks.

8. INTERCEPTION AND MONITORING

8.1. Rationale

Grindrod Shipping has a legal duty to protect and secure its facilities and networks, which include the duty to intercept and monitor Employee Communications in certain circumstances.

This Procedure aims to balance the privacy rights of employees with the security and risk management obligations of Grindrod Shipping by providing strict rules and limitations on the Interception and Monitoring of communications.

8.2. Scope of Application

This Procedure applies to all employees of Grindrod Shipping and any service providers employed to assist Grindrod Shipping in the monitoring and surveillance of employee conduct and communications.

8.3. Purpose

The purpose of this Procedure is to:

a. Provide rules for the interception of employee communications

b. Provide rules for employee surveillance

c. Balance Grindrod Shipping's security and risk management duties with the privacy and dignity rights of employees.

8.4. The Interception of Communications

8.4.1. Grindrod Shipping may only intercept and monitor communications if:

a. The employee and/or person subject to the interception or monitoring agreed thereto in writing prior to the commencement of the interception and / or monitoring;

b. Grindrod Shipping acts on the authority of a court order and/or a directive issued by the National authority.

c. The natural person conducting the interception or monitoring on behalf of Grindrod Shipping is a party to the communication, subject to interception or monitoring;

d. The interception or monitoring is incidental to the installation or maintenance of communications facilities.

8.4.2. Grindrod Shipping may only rely on the interception and monitoring rights detailed in clauses 8.4.1 a and 8.4.1 b above if:

8.4.2.1. A reasonable suspicion exists that Grindrod Shipping's communication facilities are used:

a. In a manner that threatens the security of Grindrod Shipping network

b. For illegal purposes

c. In contravention of any Grindrod Shipping policy(ies)

d. In a manner that infringes any person's privacy, copyright, personality, ownership or dignity.

8.4.2.2. The purpose of the interception or monitoring, as well as a list of potential persons who will be subject to the interception or monitoring, are provided to the Chief Executive Officer who shall:

a. Authorise or prohibit the proposed interception or monitoring

b. Authorise the proposed interception or monitoring subject to certain conditions

c. Only authorise the proposed interception or monitoring for a certain period

d. Indicate which authorised persons may execute the proposed interception or monitoring.

8.4.2.3. The actual interception and monitoring is conducted by authorised persons;

8.4.2.4. The interception and/or monitoring is conducted with due regard to the privacy, dignity and equality of the person subject to the interception and/or monitoring; and

8.4.2.5. Data collected during the interception and monitoring is collected and retained in a secure manner to prevent the unauthorised use, copying or disclosure thereof.

8.5. Data Collected Through Interception or Monitoring

8.5.1. Grindrod Shipping may only use data collected during or through interception and monitoring for legal and legitimate purposes, including as evidence in disciplinary or legal proceedings;

8.5.2. Grindrod Shipping may not disclose, use, copy or in any manner deal with data collected during or through interception and monitoring for any purpose but the purpose detailed and authorised.;

8.5.3. Data collected through interception and monitoring not relevant or applicable to the purpose detailed and authorised shall be destroyed as soon as reasonably possible after the collection and examination thereof and persons who had access thereto shall not disclose, copy or use such data in any manner;

8.5.4. All data collected through interception and monitoring shall be destroyed within four (4) years from the date upon which it was collected; and

8.5.5. Data retained for later use as evidence shall be retained in a safe and secure manner that prevents unauthorised access, tampering, destruction, disclosure or use and in a manner that maximises evidential weight .

8.6. Authorised Persons

8.6.1. Authorised persons shall be authorised to conduct Interception and Monitoring in writing by the General or Marine Manager; and

8.6.2. Authorised persons shall sign non-disclosure agreements prohibiting, amongst others, the unauthorised use, disclosure, destruction or copying of data collected during interception and monitoring.

8.7. Data Related to Communications

Communication-related information collected, retained or used by Grindrod Shipping shall be subject to the same restrictions applying to data collected during or through interception and monitoring detailed in this Procedure.

8.8. General

No employee or person with access to Grindrod Shipping's communication facilities shall develop, download, install, share, use or attempt to use any tool, device or programme to frustrate the Interception and Monitoring of communications.

8.9. Misconduct

Violation of or failure/refusal to abide by the provisions of this Procedure may result in disciplinary action and even dismissal.

9. INTERNET ACCEPTABLE USE

9.1. Purpose

This Procedure outlines appropriate and inappropriate use of Grindrod Shipping's Internet resources including the use of browsers, instant messaging, social media, peer-to-peer, file uploads and downloads and voice communications.

9.2. Social Media

Social media is defined to include, but is not limited to, any of the following:

a. Blogs
b. Chatrooms
c. Online Forums
d. Social Networks (e.g. Facebook, LinkedIn, Twitter)
e. Peer-to-Peer
f. Torrent downloads.

9.3. Streaming Media

Streaming media is defined to include, but is not limited to, any of the following:

a. Internet Video Streaming (YouTube, Sky News, etc.)
b. Internet Radio Stations
c. Instant Messaging Software which includes Voice / Video
d. Skype (unless authorised by Grindrod Shipping IT).

Access to streaming media websites is restricted on the Grindrod Shipping network. Where access is required by an employee, this needs to be applied for on an individual basis and authorised by the Marine Manager.

9.4. Your Account

Internet access at Grindrod Shipping is controlled through the user's active directory account and passwords. Business Unit Managers are responsible for defining appropriate Internet access levels for the people in their department and conveying that information to the network administrator.

9.5. Appropriate Use

Individuals at Grindrod Shipping are encouraged to use the Internet to further the goals and objectives of Grindrod Shipping. The types of activities that are encouraged include:

a. Accessing of online customer, supplier and principal applications and portals;

b. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities; and

c. Participating in educational or professional development activities as provided by Grindrod Shipping.

9.6. Inappropriate Use

Individual Internet use will not interfere with others' productive use of Internet resources. Users will not violate the network policies of any network accessed through their account. Internet use at Grindrod Shipping will comply with all local laws, all Grindrod Shipping procedures and all Grindrod Shipping contracts. This includes, but is not limited to, the following:

a. The Internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, pornography, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes and computer tampering (e.g. spreading computer viruses)

b. The Internet may not be used in any way that violates Grindrod Shipping's policies, rules or administrative orders. Use of the Internet in a manner that is not consistent with the mission of Grindrod Shipping, misrepresents Grindrod Shipping or violates any Grindrod Shipping procedure is prohibited

c. Individuals should limit their personal use of the Internet. Grindrod Shipping prohibits use for access for non-employees to Grindrod Shipping resources or network facilities, uploading and downloading of files for personal use, access to pornographic sites, gaming and competitive commercial activity, unless pre-approved by Grindrod Shipping.

d. Individuals may not establish company computers as participants in any peer-to-peer network, unless approved by management

e. Individuals will only use Grindrod Shipping-approved services for voice communication over the Internet.

9.7. Security

For security purposes, users may not share account or password information with another person. Internet accounts are to be used only by the assigned user of the account for authorised purposes. Attempting to obtain another user's account password is strictly prohibited. A user must contact the help desk or IT administrator to obtain a password reset if they have reason to believe that an unauthorised person has learned their password. Users must take all necessary precautions to prevent unauthorised access to Internet services.

9.8. Monitoring and Filtering

Grindrod Shipping may at its sole and absolute discretion, monitor any Internet activity occurring on Grindrod Shipping equipment or accounts. Grindrod Shipping currently does employ filtering software to limit access to sites on the Internet. If Grindrod Shipping discovers activities which do not comply with applicable law or departmental procedure, records retrieved may be used to document the wrongful content in accordance with due process.

9.9. Disclaimer

Grindrod Shipping assumes no liability for any direct or indirect damages arising from the user's connection to the Internet. Grindrod Shipping is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its systems. Users are solely responsible for any material that they access and disseminate through the Internet.

10. SHORT TERM LOAN OF IT EQUIPMENT

10.1. Overview

Laptop computers, 3G modems, Mobile handsets and IT peripherals are available for short-term loan from Grindrod Shipping IT. These units are not intended to replace primary work site devices, but to provide for short-term capacity constraints.

This equipment is available for use only to Grindrod Shipping employees who:

a. Need to perform work off-site

b. Need the item to perform their primary employment function while their device is being replaced or repaired.

10.2. Reservations and Handling of Equipment

All loans require approval from the Grindrod Shipping IT Services Manager . Grindrod Shipping IT cannot guarantee that a required unit will be available, since available equipment is provided on a first-come, first-served basis. An equipment loan may not exceed two (2) months and such extended request must be reviewed monthly.

10.3. Loan Period

Employees are required to report any problems experienced with the equipment during their loan period. If the loaned equipment is not returned by the predetermined deadline, the employee will be contacted and asked to return it and the employee's supervisor may be notified.

For extended loans, laptops must be inspected by Grindrod Shipping IT monthly, by the fifth (5th) of each month, to verify working condition, software updates and virus protection.

The working condition of the equipment (including all peripherals, such as cables, chargers etc.) will be assessed prior to delivery and upon its return.

10.4. IT Equipment Maintenance

All loan units are covered under the insurance. The coverage exclusions and applicable insurance excess charges are as included under the insurance procedure..

10.5. Laptop Security

Users are responsible for damage to and/or loss or theft of loaned units. In order to avoid loss or theft, please follow these guidelines:

a. **Airports**: Never leave the unit unattended. Do not check the unit as baggage. Exercise diligence in watching the unit as it passes through any x-ray devices

b. **Cars**: Keep the car locked and the unit safely stored in the boot of the vehicle. Ensure that the unit is securely stored so that it does not slide while driving. Avoid storage of the unit in a car during very hot or very cold weather. Ensure unit is well-padded to avoid external or internal damages

c. Users are responsible for performing their own data backups. Grindrod Shipping IT is not responsible for any files left on any laptop or for loss of or damage to a user's files during the loan period. Grindrod Shipping IT is also not responsible for any computer viruses transferred to or from a user's portable storage media while using the laptop.

11. MOBILE DEVICE ACCEPTABLE USE

11.1. Purpose

The purpose of this procedure is to define standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data from a mobile device connected to an unmanaged network outside of Grindrod Shipping direct control. This Mobile Device Acceptable Use Procedure applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

a. Laptop/notebook/tablet computers.

b. Mobile/cellular phones.

c. Smartphones.

d. Any mobile device capable of storing corporate data and connecting to an unmanaged network.

The procedure applies to any hardware and related software that is used to access corporate resources, even if said equipment is not corporately sanctioned, owned, or supplied.

The overriding goal of this procedure is to protect the integrity of the private and confidential client and business data that resides within Grindrod Shipping technology infrastructure. This procedure intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the company's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Grindrod Shipping direct control to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

11.2. Applicability

This procedure applies to all Grindrod Shipping employees, including full and part-time staff, contractors, freelancers, and other agents who utilise either company-owned or personally owned mobile device to access, store, back up, relocate or access any organisation or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Grindrod Shipping has built with its clients, supply chain partners and other constituents. Consequently, employment at Grindrod Shipping does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

11.3. Procedure and Appropriate Use

It is the responsibility of any employee of Grindrod Shipping who uses a mobile device to access corporate resources to ensure that all security protocols normally used in the

management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct Grindrod Shipping business be utilised appropriately, responsibly, and ethically. Failure to do so may result in suspension of that user's account.

The procedure addresses a range of threats to – or related to the use of – enterprise data:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive corporate data is deliberately stolen and sold by an employee.
Copyright	Software copied onto a mobile device could violate licensing.
Malware	Viruses, Trojans, Worms, Spyware and other threats could be introduced via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise to the risk of non-compliance with various identity theft and privacy laws.

This procedure is complementary to any previously implemented procedures dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the enterprise network.

11.4. Responsibilities

The Board of Directors of Grindrod Shipping has the overall responsibility for the confidentiality, integrity, and availability of corporate data.

Other IT, staff under the direction of the IT Manager are responsible for following the procedures within Information Technology and Information Systems.

All Grindrod Shipping employees are responsible to act in accordance with company policies and procedures.

11.5. Terminations

Users that resign from Grindrod Shipping must hand in their equipment, manuals, passwords and PUK's to the IT Department.

11.6. Connectivity

Connectivity of all mobile devices will be centrally managed by Grindrod Shipping IT department and will utilise authentication and strong encryption measures. Although IT is not able to directly manage all external devices which may require connectivity to the corporate network, end users are expected to adhere to the same security protocols when connected using non-corporate equipment. Failure to do so may result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

Grindrod Shipping IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the company's systems, data, users, and clients at risk. (See point e below)

a. Prior to initial use on the corporate network or related infrastructure, all mobile devices must be registered and be appropriately configured by Grindrod Shipping IT.

b. End users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, a company-approved personal firewall and any other security measure deemed necessary by the Grindrod Shipping IT Department.

c. All devices attempting to connect to the corporate network through an unmanaged network (i.e. the Internet) may be inspected by an identity management software tool.

   - This tool will interrogate any device attempting connection, and using predefined and configured rules, deny, grant limited or grant full access to the corporate IT resources.
   - This tool has other functions that are used in the day to day management and communication with mobile users.

d. International Data Roaming Best Practise

   - If staying in a foreign country for extended periods, purchase a local SIM card in order to obtain connection
   - at local rates
   - Make use of wireless hotspots if these are available
   - If possible, use the internet and applications such as Skype to make international telephone calls
   - When roaming, do not leave connections open when unused. Only connect when required i.e., connect, download, disconnect and then work offline
   - Turn off 3G data and use GPRS only to limit download bills

11.7. Acceptable Use

Grindrod Shipping does not restrict private use of company owned assets, however, the end user is expected to exercise restraint and use common sense when utilising company resources. Other company procedures, such as Internet Acceptable

The end user may not abuse resources to which he has been granted, such as using the company internet connection for extended periods for personal use.

Grindrod Shipping does not restrict or necessarily define which applications a user may download on his or her device. Certain applications will be recommended for specific functions. If an application attracts a fee, this will be reimbursed by the company if the application is required for business purposes. The end user takes full responsibility for maintaining full compliance with all license restrictions, terms and conditions as defined by the provider of the application / software.

11.8. Data Storage

As a generalisation, data will only be stored on private cloud servers and storage mechanisms. These central data stores are secure, managed and backed up to ensure that the integrity of the data stored here is maintained and accurate at all times. However, users may be allowed under certain circumstances to download files onto laptops and other devices when it is necessary to work offline if there is no connection medium available (e.g., during a long-haul flight). This tool may further be used to prevent a file being downloaded, if this feature is required for certain information types.

a. Data that is stored on removable media (such as memory sticks) must be encrypted and/or password protected at all times, using standards defined and software provided by Grindrod Shipping IT.

b. All data (in whatever format) will be stored on the private cloud storage device that can be accessed from anywhere at any time

c. Certain types of data files may carry additional security passwords required to open files

d. IT will use software tools to control and audit all access to data in the store

e. Access to private cloud data stores will be configured and controlled by Grindrod Shipping IT based on business requirements (as defined by the business)

- Read/write/maintain/print
- Create and delete
- Access to folders
- Notification of new documents/changes to existing data

f. Record retention policies are defined and will be applied as necessary

11.9. Collaboration

A number of tools and applications are available to users to communicate with each via data networks. Grindrod Shipping does not restrict nor dictate which tools should be used, but employees are encouraged to make use of various tools, (which may apply to specific devices only), in order to communicate. Below is a list (non-exhaustive) of elements that are available:

a. Unified messaging and Presence

b. Voice activation for control of devices

c. Facetime (available on Apple devices)

d. Skype (generally available on all devices)

- One-to-one voice and/or video (free if both units connected to internet)
- Conference (costs depend on different party connections)
- Internet to private number (prepaid, usually less than land lines)

e. Google Chat/MSN/Yahoo/LYNC/Other (text-based internet conversation)

f. IP telephony (requires software loaded)

g. Email – Grindrod Shipping standard is MS Exchange

As technology allows, Grindrod Shipping will move towards a “same number” strategy in which an employee will have a single telephone number for connection, irrespective of physical location or device that is being used at any given time.

11.10. Security

a. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password, and all data stored on the device must be encrypted using strong encryption.

b. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

c. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices.

- Grindrod Shipping may enforce the use of PIN codes on devices to prevent unauthorised access.

d. Any non-corporate computers used to synchronise with these devices will have installed anti-virus and anti-malware software deemed necessary by Grindrod

Shipping IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.

e. Passwords and other confidential data as defined by Grindrod Shipping IT department are not to be stored unencrypted on mobile devices.

f. Any mobile device that is being used to store Grindrod Shipping data must adhere to the authentication requirements of Grindrod Shipping IT department.

g. IT will manage security procedures, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Grindrod Shipping overarching security procedure.

h. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required.

i. In the event of a lost or stolen mobile device it is incumbent on the user to report this to Grindrod Shipping IT immediately. The device will be remotely wiped of all data (including both company and private data) and (if possible) locked to prevent access by anyone other than Grindrod Shipping IT. If the device is recovered, it can be submitted to Grindrod Shipping IT for re-provisioning.

j. If it is a business requirement, GPS enablement can be enforced and allow full and visible tracking of the device at all times.

11.11. Help & Support

Grindrod Shipping IT department will support its sanctioned hardware and software but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the Grindrod Shipping IT department.

Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of Grindrod Shipping IT department. This includes, but is not limited to, any reconfiguration of the mobile device.

Grindrod Shipping IT reserves the right, through procedure enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

11.12. Organisational Protocol

Grindrod Shipping IT can and will establish audit trails and these will be accessed, published and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or

misuse. The end user agrees to and accepts that his or her access and/or connection to Grindrod Shipping networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains Grindrod Shipping's highest priority.

The end user agrees to immediately report to his/her manager and Grindrod Shipping IT department any incident or suspected incidents of unauthorised data access, data loss, and/or disclosure of company resources, databases, networks, etc.

11.13. Procedure Non-Compliance

Failure to comply with the Mobile Device Acceptable Use Procedure may, at the full discretion of the organisation, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

The immediate Manager will be advised of breaches of this procedure and will be responsible for appropriate remedial action which may include disciplinary action, including suspension or termination of employment.

Any questions relating to this procedure should be directed to Grindrod Shipping IT Department. Contact details can be found in Emergency Contact Details.

12. PASSWORD

12.1. Rules

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Grindrod Shipping's entire corporate network. All Grindrod Shipping employees (including contractors and vendors with access to Grindrod Shipping systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

This Procedure seeks to ensure that a standard for the creation of strong passwords is established and that passwords are protected and changed frequently.

12.2. Rules

a. All system-level passwords except domain service accounts (e.g. root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

b. All production system-level passwords must be part of the InfoSec administered global password management database.

c. All user-level passwords (e.g. email, web, desktop computer, etc.) must be changed every seventy (70) days.

d. The system will not allow you to repeat the last ten (10) passwords used.

e. The system will not allow a blank password.

f. Minimum password age is nil (0) days.

g. Maximum password age is seventy (70) days.

h. User accounts that have system-level privileges granted through memberships must have a unique password from all other accounts held by that user.

i. Passwords must not be inserted into email messages or other forms of electronic communication.

j. Passwords must be a minimum of six (6) characters long.

k. The use of capitalisation, numbers and at least one (1) special character in the password is encouraged, but not enforced.

l. All user-level and system-level passwords must conform to the guidelines described below.

12.3. Guidelines

Passwords are used for various purposes including:

a. user-level accounts

b. web accounts

c. email accounts

d. application login

e. screen saver protection

f. voicemail password.

Since very few systems have support pass-through authentication (i.e. dynamic passwords which are only used once), the following guidance should be considered when selecting passwords:

12.3.1. Poor Passwords

Poor, weak passwords have the following characteristics:

a. The password contains less than five characters

b. The password is a word found in a dictionary (English or foreign)

c. The password is a common usage word such as:

d. Names of family, pets, friends, co-workers, fantasy characters, etc

e. Computer terms and names, commands, sites, companies, hardware, software

f. The words “GRINDROD SHIPPING”, “SHIPPING”, “TRADE”, “UNICORN”, etc or any derivation of Grindrod Shipping company names

g. Birthdays and other personal information such as addresses and phone numbers

h. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc

i. A combination of the current calendar month and year e.g. april2011

j. Any of the above spelled backwards

k. Any of the above preceded or followed by a digit (e.g. secret1, 1secret).

12.3.2. Strong Passwords

Strong passwords have the following characteristics:

a. Contain both upper and lower-case characters (e.g. a-z, A-Z)

b. Have digits and punctuation characters as well as letters e.g. 0-9, !@#$%^&*()_+|~- =\`{}[]:”;’<>?,./)

c. Is not a word in any language, slang, dialect, jargon, etc

d. Are not based on personal information, names of family, etc

e. Passwords should never be written down or stored on-line

f. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: “This May Be One Way to Remember” and the password could be: “TmB1w2R!” or “Tmb1W>r~” or some other variation.

12.3.3. Protection Standards

Do not use the same password for Grindrod Shipping accounts as for other non-Grindrod Shipping access (e.g. personal ISP account, option trading, benefits, etc.). Where possible, don’t use the same password for various Grindrod Shipping access needs. For example, select one (1) password for each application system and a separate password for mail systems. Do not share Grindrod Shipping passwords with anyone, including administrative assistants or secretaries.

12.4. Password Don’ts

All passwords are to be treated as sensitive, confidential GRINDROD SHIPPING information.

a. Don't reveal a password over the phone to ANYONE
b. Don't reveal a password in an email message
c. Don't reveal a password to the boss
d. Don't talk about a password in front of others
e. Don't hint at the format of a password (e.g. "my family name")
f. Don't reveal a password on questionnaires or security forms
g. Don't share a password with family members
h. Don't reveal a password to co-workers while on vacation
i. If someone demands a password, refer them to this document or have them call someone at the IT Call Centre
j. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including PDAs, Smartphones or similar devices) without encryption
k. Change passwords at least once every four (4) weeks (except system-level passwords which must be changed quarterly). If an account or password is suspected to have been compromised, report the incident to IT Call Desk immediately and change all passwords
l. Password cracking or guessing may be performed on a periodic or random basis by IT or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

12.5. Application Development Standards

Application developers must ensure their programmes contain the following security precautions:

a. Support authentication of individual users, not s
b. Do not store passwords in clear text or in any easily-reversible form
c. Provide role management, such that one user can take over the functions of another without having to know the other's password
d. Support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible. Use of Passwords and Passphrases for Remote Access Users.

13. PRINTER

13.1. Purpose

This Procedure facilitates the appropriate and responsible business use of Grindrod Shipping's printer assets, as well as control Grindrod Shipping's printer cost of ownership by preventing the waste of printer consumables.

13.2. Supported Printers

Grindrod Shipping supports a wide variety of printers, however before procuring a new printing device, IT must be consulted to confirm that the correct device is being procured for the desired usage and where possible effort will be made to standardise on specific printer models in order to optimise contractual agreements and minimise support costs. T

13.3. General Procedure

13.3.1. Printers are to be used for documents that are relevant to the day-to-day conduct of business at Grindrod Shipping. Printers should not be used to print personal documents.

13.3.2. The general procedure is that network printers (MFP's) will be used as departmental printers, serving a of people simultaneously. Where required, multi-functional networked printers will be used as photocopiers and facsimile machines and will be linked to email so that a document can be scanned and emailed without the need to print additional copies.

13.3.3. Installation of personal printers is generally not allowed due to the operating cost of these devices. In certain circumstances, however, where confidentiality, remote location, the need to print a large number of low volume print jobs or other unusual situations are an issue, personal printers may be allowed.

13.3.4. Multiple copies of the same document must not be printed – the printer is not a copier and costs more per page to use. If you need multiple copies, print one good copy on the printer and use the photocopier to make additional copies.

13.3.5. If you print something to a shared printer, pick it up in a timely fashion. If you no longer want it, please dispose of it appropriately (i.e. recycle).

13.3.6. Unclaimed print jobs on the MFP unit must be stacked neatly alongside the printer and will be discarded after two (2) days into the paper recycling bin.

13.3.7. Limit paper usage by taking advantage of duplex printing (i.e. double-sided printing) features offered by some printers and other optimisation features (e.g. printing six (6) PowerPoint slides per page versus only one (1) per page).

13.3.8. Limit toner use by selecting light toner and lower dpi default print settings.

13.3.9. Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer. Please report any planned print jobs in excess of one hundred (100) pages to the IT department so that the most appropriate printer can be selected and other users can be notified.

13.3.10. Avoid printing email messages, this is wasteful. Instead, use the folders and archiving functionality in your email application to organise and view your messages.

13.3.11. Avoid printing a document just to see what it looks like. This is wasteful.

13.3.12. Avoid re-using paper in laser printers, as this can lead to paper jams and other problems with the machine.

13.3.13. Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper.

13.3.14. Colour printing is typically not required by general business users. Given this selective need, as well as the high cost per page to print colour copies, you are strongly encouraged to avoid printing in colour when monochrome (black) will do.

13.3.15. Only genuine toner cartridges may be used in printers that are still under warranty. Refills and refurbished cartridges are discouraged as physical damage can occur to the printer unit. However, the decision to use these cartridges on printers out of warranty remains with the affected business unit who acknowledges the possible damage that may occur and accepts that any costs directly related to subsequent repairs or servicing are for their direct account.

14. SERVER SPACE

14.1. Overview

This Procedure is designed to curtail the increasing use of company server space for unauthorised, non-business-related files, preserving the finite amount of storage space available on network servers.

14.2. Appropriate Files for Storage

Files that directly pertain to the business of Grindrod Shipping may be saved on a network server or appropriate SharePoint drive. These include most business files created through the use of IT Department-approved and installed software.

Inappropriate files include non-business-related audio files, non-business-related video files, image files, games, executables, script files and any other employee-installed software not approved by the IT Department. Not only do such files consume valuable server space, but they can also introduce damaging viruses into the network.

Attempts will be made to block the storage of all non-business-related files. If such files are detected on the server, you will be asked to remove them immediately.

14.3. Tips for Conserving Storage Space

It is the responsibility of every employee to ensure that they use their server storage space allocation wisely. Each employee should set aside time on a monthly basis to ensure that they remain within their space quota. Identify, remove and/or archive items that are:

a. Outdated, such as preliminary draft versions of current documents
b. Out-of-use or orphaned files
c. Duplicated files
d. Non-business-related or non-critical files.

15. SOCIAL MEDIA AND ELECTRONICS COMMUNICATION PROCEDURE

15.1. Introduction

The effective use of Social Media and Electronic Communication can be extremely beneficial to any organization. Therefore, this document is aimed at empowering our employees to use these emerging technologies responsibly.

For the purposes of this Procedure, social media means any facility for online publication and commentary. Including and not limited to blogs, wiki's, social networking sites such as Facebook, LinkedIn, Twitter, Flickr, You Tube, Vimeo, Ning, and any electronic means of publishing or communicating through electronic means, including e-mail and skype. This Procedure is in addition to and complements the company's Corporate Governance policies and procedures and the company's procedures regarding the use of technology, computers, smart phones, electronic communication devices, e-mail or the internet.

This procedure applies to all employees (including consultants) when they publish comment or communicate through social media or electronic communication methods.

15.2. Personal use of Social Media

When using personal social media, Company Employees should be aware, they are not authorized to post information relating to the Company or to represent the company or express a view on behalf of the Company.

Employees are free to set up and use any form of social media within the given framework of the terms provided by the host of such spaces. However, it is important that their personal participation in social media does not interfere with their primary role at Grindrod Shipping.

Be aware of your association with the Company in online social networks. Ensure that your profile and related content is consistent with how you wish to present yourself with colleagues, clients, partners or suppliers.

If you decide to use any form of social media and make reference to Grindrod Shipping, please use this disclaimer:

"Postings on this space belong to (Enter Name Here) and only contain my personal positions, strategies and opinions. It is not endorsed by Grindrod Shipping or its subsidiary companies nor does it constitute any official communication of Grindrod Shipping or its subsidiary companies."

15.3. Work-Related Social Media

Before engaging in work-related social media, please obtain written permission from the business unit CEO and register with the ethics committee as a social media administrator. When posting information, company employees should ensure that they conduct themselves in a way which reflects positively on the Company.

When communicating via e-mail or skype or participating in Social Media on behalf of Grindrod Shipping or a subsidiary company, please be aware that you are representing the company in the same way as you would in any other public forum.

Therefore, it is important to adhere to the following guiding principles:

a. Grindrod Shipping's Code of Conduct;
b. Grindrod Shipping's Confidentiality Obligations – Do not post proprietary information and/or content unless you have permission to do so. Never discuss the company's business performance, sales data or plans, finances, legal matters or other matters considered confidential;
c. The "Terms of Use" of third party sites;
d. Respect copyright laws;
e. The local legal and ethical regulations;
f. Identify yourself, write in the first person;
g. Do not make false or misleading comments/statements. If you have made a mistake, take responsibility for it;
h. Do not use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the company workplace;

i. Exercise discretion and confidentiality when referring to your colleagues and customers. Do not cite or reference clients, colleagues, partners or suppliers without their approval. Do not publish any information that may embarrass or damage the Company, a client, colleague, partner or supplier;

j. Stick to what you know, post meaningful comments, and aim for quality;

k. Be diligent and check your sources, separate opinions from facts and identify all copyrighted or borrowed material with citations and links;

l. Stay engaged and informed. Post regularly, and respond to comments in a timely manner;

m. Protect your privacy and never disclose your personal information;

n. Use Common Sense – Once it's posted it's there for good. Be sure to review your posts thoroughly and "spell check" everything.

15.4. Moderation & Media

The Company reserves the right, but is not obligated, to moderate content posted by you on work-related media. The Company also reserves the right to monitor any social media and any social media usage for the compliance with this Procedure. Employees should be aware that they have no expectation of privacy whatsoever when communicating via social media for, about or in relation to (1) their employment, (2) the Company, or (3) the Company's business.

Media Inquiries – Your contributions to social computing and online conversations might attract media attention. If a member of the media contacts you, simply notify the Media Relations team via Grindrod Shipping@Grindrod Shipping.co.za They will determine the best way to handle the inquiry.

Violations of this Procedure will be subject to disciplinary action, up to and including termination for cause.

16. SUPPORT

16.1. Purpose

Grindrod Shipping IT provides computer and information systems support for all employees. This Procedure sets out the basic level of service that will be guaranteed by the IT Department and identifies and delineates the limits of IT's capabilities and what will not be supported.

16.2. Scope

"IT support" is defined as any queries made by end users to the IT Department regarding any failures, problems, issues, questions and other matters relating to the operation and continuity of company-owned PCs, servers, websites, software, peripherals, telephony, mobile devices and other IT equipment or assets.

The range of support offered and guaranteed by the IT Department will vary depending on the nature of the problem, the number of staff or resources available to resolve the problem, the criticality of the asset in question and other factors regarding the nature of the support requested.

16.3. Contact

The IT support team can be contacted in a variety of methods:

a. An email message to shippingsupport@Grindrod Shipping.co.za, (preferred method) fully describing the problem

b. Via telephone (Details found on the Emergency Contact List.)

16.4. Service Offering

16.4.1. Software Support

Support is provided for all core software packages and operating systems on Grindrod Shipping workstations, servers, laptops, and other computing equipment. Support is also provided for department-specific software applications. The supported list of software is available from the IT department on request. Please note that personally installed or unlicensed software, including screensavers, games, applications whose publishers are no longer in business, etc., will not be supported by the IT Department. Unauthorised installation of software is illegal and in violation of other Grindrod Shipping policies. Unauthorised and illegal software will be removed immediately by IT and may not be reinstalled by the user.

16.4.2. Hardware Support

Support is provided for all core hardware and devices, including PC motherboards, peripherals, network interface cards, hard drives, storage devices, and so on. All cases of suspected hardware faults will be diagnosed accordingly. The IT Department will attempt to fix hardware defects to the best of its ability but may need to send equipment back to the vendor/manufacturer. Wherever possible, replacements will be found for the end user in such cases. Please note that personally installed or unapproved hardware, including speakers, unauthorised monitors, personal cell phones, etc. will not be supported by the IT Department.

Unauthorised installation of hardware is illegal and in violation of other Grindrod Shipping procedures.

16.4.3. Remote Support

All remote access will be managed by Grindrod Shipping's IT using encryption and strong authentication measures. Remote access connections covered by this Procedure include (but are not limited to) VPN connections via any medium and via 3G utilising the Grindrod Shipping Private APN.

16.4.4. Determining Support

Telephone support will be the mode of choice for most minor problems and difficulties. The IT Department will conduct on-site support at the end user's workstation where applicable. On-site support will be provided for teleworkers or mobile workers who are within a reasonable driving distance from the office. For distant offices and working areas, support will be provided by IT appointed sub-contractors in the applicable area. Otherwise, telephone support will be provided, unless the user is able to bring the equipment in for inspection as prearranged with IT. Walk-in support is generally not provided without an appointment, but exceptions will be made in emergency situations, and these will be assessed on a case-by-case basis.

16.4.5. Enforcing Support

The IT Department reserves the right to monitor hardware and software installation and usage on Grindrod Shipping's computer systems. The IT Department will conduct periodic audits to ensure compliance with this IT Support Procedure. Unannounced, random spot audits may be conducted as well. During such audits, scanning for and removal of rogue software and hardware will be performed.

16.4.6. Personal Support

Support will not be granted for personally-owned software and hardware. In cases where a business case can be made for an employee using personal equipment for Grindrod Shipping purposes (e.g. via a teleworking or telecommuting arrangement) and is authorised by the employee's line Manager, support may be granted. End users agree not to approach any IT staff member for the purpose of soliciting support for personally owned hardware and/or software. The urgency of personal support will not supersede the urgency of other business-related support.