IT EMAIL AND WEBSITE POLICY

HA GROUP LTD

54 Andries Street
Wynberg, Sandton,
Republic of South Africa
GP, 2090

POLICY NAME	IT EMAIL AND WEBSITE POLICY			**POLICY NO.**	202300001
EFFECTIVE DATE	21/02/2023	**DATE OF LAST REVISION**	09/12/2024	**VERSION NO.**	202400002

ADMINISTRATOR RESPONSIBLE	CLARENCE ITAI MSINDO	**CONTACT INFORMATION**	+27 68 065 5718

VERSION HISTORY

VERSION	APPROVED BY	REVISION DATE	DESCRIPTION OF CHANGE	SIGNATURE
202300001	Dr. Clem Msindo	N/A	Establishment	
202400001	Clarence Itai Msindo	15/02/2024	Website Register & Email Security	Msindo
202400002	Clarence Itai Msindo	09/12/2024	Website Content, Website Register, Backup Email System.	Msindo

TABLE OF CONTENTS

INTRODUCTION

HA GROUP LTD makes all resources available to its employees where relevant and useful for their jobs. This policy describes the rules governing the use of technology at the company. It also sets out how staff members are expected to behave when using IT resources.

SCOPE

This policy applies to all staff, contractors, and key stakeholders at **HA GROUP LTD**.

EMAIL POLICY

PURPOSE OF THE POLICY

Email is a standard way to communicate in business. It's used widely and is arguably
just as important as the telephone. Like any technology, email can cause difficulties if used incorrectly or inappropriately. This email policy:

- Reduces the security and business risks faced by **HA GROUP LTD**.
- Lets staff know how they are permitted to use company email.
- Ensures employees follow good email etiquette.
- Helps the company satisfy its legal obligations regarding email use.

GENERAL EMAIL GUIDELINES

BUSINESS EMAIL USE

HA GROUP LTD recognises that email is a key communication tool. It encourages its employees to use email whenever appropriate. For instance, staff members may use email to:

- Communicate with customers or suppliers.
- Market the company's products.
- Distribute information to colleagues.

PERSONAL USE OF EMAIL

The company also recognises that email is an important tool in many people's daily lives. As such, it allows employees to use their company email account for personal reasons, with the following stipulations:

- Personal email use should be of a reasonable level and restricted to nonwork times, such as breaks and during lunch.
- All rules described in this policy apply equally to personal email use. For instance, inappropriate content is always inappropriate, no matter whether it is being sent or received for business or personal reasons.
- Personal email use must not affect the email service available to other users. For instance, sending exceptionally large files by email could slow access for other employees.
- Users may access their own personal email accounts at work if they can do via our internet connection. For instance, a staff member may check them Yahoo or Google Mail during their lunch break.

AUTHORISED USERS

Only people who have been authorised to use email at **HA GROUP LTD** may do so. Authorisation is usually provided by the company Systems Administrator. It is typically granted when a new employee joins the company and is assigned their login details for the company IT systems. Unauthorised use of the company's email system is prohibited. Employees who use company email without authorisation — or who provide access to unauthorised people — may have disciplinary action taken against them. The disk space allocated to all employees except country managers and Projects CEO will be 1GB each.

KEY AREAS

EMAIL SECURITY

Used inappropriately, email can be a source of security problems for the company. Users of the company email system must not:

• Open email attachments from unknown sources, in case they contain a virus, Trojan, spyware or other malware.
• Disable security or email scanning software. These tools are essential to protect the business from security problems.
• Send confidential company data via email. The Systems Administrator can advise on appropriate tools to use instead.
• Access another user's company email account. If they require access to a specific message (for instance, while an employee is off sick), they should approach the Projects Director or the Systems Administrator.

Staff members must always consider the security of the company's systems and data when using email. If required, help and guidance is available from the Systems Administrator. While email security has improved, and many systems encrypt messages in transit, **no system is entirely immune to interception**. Be cautious with confidential messages and use the provided secure communication methods for sharing sensitive information.

INAPROPRIATE EMAIL CONTENT AND USE

The company email system must not be used to send or store inappropriate content or materials. It is important employees understand that viewing or distributing inappropriate content via email is not acceptable under any circumstances. Users must not:

• Write or send emails that might be defamatory or incur liability for the company.
• Create or distribute any inappropriate content or material via email. Inappropriate content includes pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling, and illegal drugs. This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone based on race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
• Use email for any illegal or criminal activities.
• Send offensive or harassing emails to others.
• Send messages or material that could damage **HA GROUP LTD**'s image or reputation. Any user who receives an email they consider to be inappropriate should report this to the Systems Administrator or Projects Director.

COPYRIGHT

HA GROUP LTD respects and operates within copyright laws. Users may not use company email to share any copyrighted software, media or materials owned by third parties, unless permitted by the company. Employees must not use the company's email system to perform any tasks that may involve breach of copyright law. Users should keep in mind that the copyright on letters, files and other documents attached to emails may be owned by the email sender, or by a third party. Forwarding such emails on to other people may breach this copyright. Please take note of the following policies regarding **HA GROUP LTD**'s branding and logo:

- **HA GROUP LTD**'s logo and branding are the company's intellectual property and must not be used without prior approval.
- Users may not use **HA GROUP LTD**'s logo or branding to associate with any content or activity that may bring reproach to the company.
- The company's logo and branding must not be used in any social media post or website content that violates copyright laws or infringes on the rights of others.
- Employees must ensure that any images or other content used on the company's website or social media platforms are either owned by the company or are used with permission and do not violate any copyright laws.

- Any use of **HA GROUP LTD**'s logo or branding must be in accordance with the company's brand guidelines, which can be obtained by contacting the company.

CONTRACTS AND LIABILITY

Users must be careful about making commitments or agreeing to purchases via email. An email message may form a legally-binding contract between **HA GROUP LTD** and the recipient — even if the user has not obtained proper authorisation within the company.

EMAIL MARKETING AND BULK EMAIL

HA GROUP LTD may use email to market to existing and potential customers. There is significant legislation covering bulk email and use of email for marketing. All email campaigns must be authorised by the company and implemented using the company's email marketing tool. Users must not send bulk emails using the standard business email system. All questions about email marketing should be directed to the company.

EMAIL BEST PRACTICE

EMAIL ETIQUTTE

Email is often used to communicate with customers, partners and other important contacts. Although a relatively informal medium, staff should be aware that each email they send does affect the company's image and reputation. It's a good idea to follow rules of good email etiquette. Users must:

- Not forward on chain emails or 'humorous' messages. This clogs up people's in-boxes and some topics are not appropriate for the workplace.
- Always use a meaningful subject line rather than leaving it blank or using a single word like 'hello'.
- Only use the 'important message' setting sparingly, for messages that really are important.
- Never ask recipients to send a 'message read' receipt. Many people find these annoying and not all email services support them.
- Not use ALL CAPITAL LETTERS in messages or subject lines. This can be perceived as impolite or shouting.
- Be sparing with group messages, only adding recipients who will find the message genuinely relevant and useful.
- Use the 'CC' (carbon copy) field sparingly. If someone really needs to receive a message, they should be included in the 'to' field.
- Use the 'BCC' (blind carbon copy) field to send group messages where appropriate. It stops an email recipient seeing who else was on the email.

INTERNAL EMAIL

Email is a valid way to communicate with colleagues. However, it tends to be overused for internal communication. Users should keep these points in mind when emailing colleagues:

- Would the issue be better addressed via a face-to-face discussion or telephone call?
- Is email the best way to send a document out for discussion? Often, it becomes very hard to keep track of feedback and versions.
- It's rarely necessary to 'reply all'. Usually, it's better to reply and then manually add other people who need to see a message.

POLICY ENFORCEMENT

MONITORING EMAIL USE

The company email system and software are provided for legitimate business use. The company therefore reserves the right to monitor employee use of email. Any such examinations or monitoring will only be carried out by authorised staff. Additionally, all emails sent or received through the company's email system are part of official **HA Group LTD** records. The company can be legally compelled to show that information to law enforcement agencies or other parties. Users should always ensure that the business information sent via email is accurate, appropriate, ethical, and legal.

POTENTIAL SANCTIONS

Knowingly breaching this email use policy is a serious matter. Users who do so will be subject to disciplinary action. Employees, contractors, and other users may also be held personally liable for violating this policy. Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy. However, the company is unlikely to take formal action if a user fails to adhere to the guidelines in the 'email best practice' section.

EMAIL AND WEBSITE SECURITY POLICY

PURPOSE OF THE POLICY

The purpose of the policy is to minimize risk associated with website and e-mail services, and defines controls against the threats of unauthorized access, theft of information, theft of services, and malicious disruption of services.

PROCEDURES

PASSWORDS

All user-level and system-level passwords are generated automatically from the server. All user passwords are kept by the Systems Administrator. Passwords must not be shared with anyone. All passwords are to be treated as sensitive and confidential information. Any user suspecting that his/her password may have been compromised must report the incident to the Systems Administrator and change the password. All user-level and system-level passwords will be changed at least every year. They will be automatically generated and is passed on from the Systems Administrator. If the user does not receive the new password at the time, he/she must get in touch with the Systems Administrator *(server_admin@hpcagroup.africa)*. If the Systems Administrator does not respond instantly, you may get in touch with the Projects Director (*clem@hpcagroup.africa*).

WEBSITE POLICY

PURPOSE OF THE POLICY

To outline who will be responsible for the maintenance of the website if need be.

WEBSITE CONTENT

The website content will only be changed by the Systems Administrator. If there is need for more content or a suggestion, please let the Systems Administrator know with the email address *server_admin@hpcagroup.africa* . The website is secured and protected although we cannot guarantee that is 100% safe. To maintain content accuracy and relevance, a bi-annual review process is conducted where department heads verify their respective information, ensure contact details are current, and identify any content that needs to be archived. The website must consistently adhere to company branding guidelines, maintain mobile compatibility across all pages, project a professional image, and carefully protect confidential information. Content changes are evaluated based on these standards before implementation.

WEBSITE REGISTER

The website is registered as follows:

Domain: hpcagroup.africa
Registrar: DNS Africa Ltd
Registered On: 2022-04-28
Expires On: 2025-04-28
Updated On: 2024-04-14

BACKUP AND RECOVERY POLICY

PURPOSE OF THE POLICY

The purpose of this policy is to provide means to:

1. Restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster; and
2. provide a measure of protection against human error or the inadvertent deletion of important files.

POLICY

- All user-level and system-level information maintained by **HA GROUP LTD** shall be backed up periodically. The backup media shall be stored with enough protection and proper environmental conditions.

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.

- Any vendor(s) providing offsite backup storage for must be cleared to handle the highest level of information stored.

- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest sensitivity level of information stored.

- Backup copies of operating systems and other critical information system software shall not be stored in the same location as the operational software.

- The system backup information shall be provided with protection from unauthorized modification and environmental conditions.

- Backups must be periodically tested to ensure that they are recoverable. To confirm media reliability and information integrity, the back-up information shall be tested at some specified frequency.

- Signature cards held by the offsite backup storage vendor(s) for access to backup media must be reviewed annually or when an authorized individual leaves **HA GROUP LTD.**

- Backup information shall be selectively used to restore information system functions as a part of business continuity process.

- Procedures between **HA GROUP LTD** and the offsite backup storage vendor(s) must be reviewed at least annually.

- Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
  a. System name
  b. Creation Date
  c. Sensitivity Classification [Based on applicable electronic record retention regulations.
  d. Contact Information

BACKUP EMAIL SYSTEM

HA GROUP LTD will maintain a backup email system that will be activated in the event of an email server outage. The backup email system will be accessible to all authorized employees and will provide basic email functions, including sending and receiving emails. Take note of the following policies:

- **Use of Gmail as Backup Email**: If the company's email system is down, employees should use a Gmail account as a backup email. The format for the Gmail account should be "***[yourname].hpcagroup@gmail.com***". The use of Gmail should be limited to backup purposes only and employees should not use the account for any other business-related activities.

- **Access to the Backup Email System**: All employees with authorized access to the company's email system will also have access to the backup email system. If employees have trouble accessing the backup email system, they should contact the Systems Administrator for assistance.

- **Main email system outage**: In the event of main email system failure, users should switch to their Gmail backup account and immediately notify the Systems Administrator, following documented recovery procedures until the main email system is restored. The Systems Administrator will conduct yearly backup checks, while users are required to test their Gmail backup access quarterly.

- **Email Functions on the Backup Email System**: The backup email system will provide basic email functions, including sending and receiving emails. However, employees may not have access to email archives or attachments during the outage.

- **Switching Back to the Main Email Server**: Once the main email server is operational again, the Systems Administrator will evaluate the readiness of the main email server to resume normal operations. The Systems Administrator will then communicate the switch back to the main email server to all employees, along with instructions for transferring any data from the backup email system back to the main server.

- **Communication**: All employees will be notified of the activation of the backup email system and the switch back to the main email server via email or another communication channel.

- **Testing and Updating**: The backup email system will be regularly tested and updated to ensure that it is ready for use in the event of an email server outage.

- **Compliance**: All employees are expected to comply with this policy to ensure continuity of business operations in the event of an email server outage.

ENFORCEMENT

Any employee found to have violated this policy may be subjected to disciplinary action.