NASE Information Security and Data Protection Policy

AUTHOR:

Dennis Aguma
Executive Director, NASE
E: aguma@nase.co.ug | www.nase.co.ug
T: +256776696500 | +256708080008 | +447951212772

Privileged and Confidential | Adopted on 31st January 2020

TABLE OF CONTENTS

1.0. INTRODUCTION

This policy covers the following:

1. Data protection
2. Duty of care/ security
3. Information technology/ data security
4. Privacy policy
5. Data retention policy

Purpose:

NASE has an obligation to secure the information provided to us by our people and our customers as well as the information that supports our continued growth and success. It is everyone's responsibility to protect all information assets and to adhere to the Company's information security policies.

The Company's information management system will ensure appropriate security controls across the business and commitment to the continual improvement of our information security management system.

2.0. POLICY: Data Protection and Information Security

All information handled by the Company, both physical and electronic, must be appropriately secured to protect against the consequences of a breach of confidentiality, failures of integrity, or interruptions to their availability.

The information security objective is aligned with the Company's strategy, core values and based on the following principles.

a. Proactive Risk Management

b. Protecting Company and customer information

c. Cyber security considered in technology decisions;

d. Training our people to understand threats;

The Head of Administration will ensure these principles, review them annually and progressively report to the leadership team.

3.0. POLICY: Information Technology and Data Security

Policies on Use of IT Equipment and Systems including but not limited to; servers, laptops, desktops, mobile / landline phones and any mobile storage devices such as USB sticks)
Staff and contractors must not:
Process or store Company data on non-Company issued devices

a. Share log-in or password details. You are responsible at all times for any activity logged against your user ID or password

b. Leave computers logged in when they are unattended

c. Use the Company's equipment for activities that have a negative impact on the day-to-day functioning of the business (e.g., streaming high bandwidth video / computer games)

d. Use the internet, email or instant messaging applications for the purposes of harassment or abuse

e. Use profanity, obscenities or derogatory remarks in any form of communication

f. Use the Company's resources to conduct personal business ventures

4.0. POLICY: Use of the Company's software / applications

Staff must use only software authorised by the Company on the Company's equipment. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on the Company's equipment must be approved and installed by IT.

You must not:

a. Remove or disable software without prior approval from IT

b. Upload, download, install or otherwise transmit commercial software or any copyrighted materials belonging to parties outside the Company, or the Company itself without the approval of IT.

IT must be contacted immediately should a virus be suspected on Company issued equipment.

5.0. POLICY: Duty of Care

Staff must protect all data and information received in the course of conducting business and operations.

You must not:

a. Forward Company emails or data to personal email accounts (e.g. a Gmail account) or open any unexpected/unfamiliar email attachment(s), or embedded links, as they may contain viruses, worms or unauthorised software applications. Note: If unsure check with the sender first.

b. When sending/receiving emails it is important to: only send to the intended recipients. External recipients are identified as such and highlighted as being outside the Company. You must check email addresses are correct before sending.

c. Not use personal or external email accounts to conduct the Company's business

d. Not auto-forward Company emails to personal or external email accounts

e. Not reveal or publicise confidential or proprietary information.

f. Place any information on the internet that relates to the Company and customers unless specifically authorised to do so.

6.0. PRIVACY

This policy applies to all staff and contractors. It is the responsibility of each individual to review, understand and comply with this policy. Recording meetings has the following legal implications:

a. Consent needs to be obtained from those being recorded including any attendees who are late. Lack of consent could lead to a breach of privacy.

b. Recordings would be stored on the Company's drives where there is no process for deletion when they are no longer required. This could result in a breach of privacy.
c. Recordings would be disclosable in legal proceedings and in a response to a subject access request.

This policy covers the use of both audio and/or visual technology to make recordings, in person and remotely.

POLICY

a. Recording of meetings with customers is not permitted.
b. Covert recording of meetings is prohibited and to do so will be considered a disciplinary matter.
c. However, where a customer asks or agrees to record a meeting, we can agree to this provided the recording will be deleted when it is no longer required.

7.0. DATA RETENTION

a. Restricted and Confidential information must be disposed of securely to minimise the risk of disclosure. Hard copies of information must be placed in a confidential waste bin when no longer required.
b. Destruction of electronic information must be undertaken as soon as it is no longer required. Company issued equipment such as laptops, mobile phones and USB keys that are no longer required must be returned to IT/Administration. who can remove the information stored on them.

8.0. BREACH OF THIS POLICY

Any member of NASE' staff who is found to have acted in breach of this Policy will be subject to disciplinary action, which may lead to the member of staff's dismissal.

– END –

This NASE Information Security and Data Protection Policy has been reviewed and is recommended for approval by:

……

Dennis Aguma
Executive Director, NASE
E: aguma@nase.co.ug | www.nase.co.ug
T: +256776696500 | +256708080008 | +447951212772

Privileged and Confidential
Last Updated on 31st March 2021.