NOBLE USE SERVANTS EVANGELISISM TEAM AND ASSOCIATES

INFORMATION SYSTEMS AND MEDIA/COMMUNICATION POLICY

Table of Contents

1 Introduction

This document contains the general guidelines to the usage, development and implementation of the Information systems that are owned, bought or leased by NUSETA.

It guides the operations of the National ICT Committee (NICTC)

2. The National ICT Committee (NICTC):-

a) Shall be composed of the ICT Director and seven other members appointed by the NEB from chapter executive committee members with ICT literacy and or other non-executive members, non-students or associates with similar qualifications, comprising of:
   i) Chief Editor
   ii) Communications secretary- shall be in charge of physical welfare of the IT and Media assets. Shall be in charge of communication.
   iii) Treasurer
   iv) Four other designers
b) Shall manage, maintain and control the use of electronic and print media belonging to the team
c) Shall ensure proper facilitation, recording and transmission of e-media during the team's services.
d) Shall propose, prepare and present literature materials for the use by the team
e) Shall ensure update of the website and magazine with articles and literature

f) They shall outsource from within the lager NUSETA, IT and media experts to serve as need arises in designated areas of operation.

g) Shall advertise the Editorial and Literature ministry and run its operations.

3. Information Management Policies

3.1 Creation

- Creation of any media should be done by the approval of ICT director and the NEB
- The password and recovery details uploaded in the team repository and follow the file naming process
- For accounts allowing multiple administrators, access should be given to at least two people, priority to the NICTC or other personnel recommended by the NICTC based on relevance.
- Clear indication of the objectives intended to be achieved, working/operation, features and the creating/development process should be done in writing to the NEB through the ICT director, upon approval the developing party will proceed to develop the accounts/platforms and issue final report about the work.
- A periodic update should be done to the accounts to avoid dormancy

3.2 Uploading content

- All platforms should be clearly declared open or restricted for members.
- In the case of open platforms(where members can freely share) a clear guideline on the usage should be made by the NICTC
- Content should be reviewed by the NICTC first before posting, if content is coming from the members a clear email or other media trail should be maintained.
- In the incident of faulty content or message on any of the Teams platforms, an official corrective communication should be done through the same channel by the ICT Director for the NEB.

3.3 Deleting/Terminating accounts

- Approval should be given from the NEB in writing through the ICT Director

3.4 Data collection and issuance

- Request of any data from the national repository and databases should be done to the NEB through the ICT director in writing or through formal email.

3.5 communication

No content shall be uploaded on the team's website without approval by the NICTC, subject to review by the NEB

Any content must comply with the doctrinal statement of the team's constitution and of sound doctrine.

All members who wish to post their content shall do so through the NICTC

All official communications shall be done through the NICTC.

The NEB, chapter or Cell Leadership using official channels of communication shall only use the given platforms through, or by the approval of the NICTC

3.6 Repository and storage

- A National Central accessible Repository shall be maintained.
- The National Repository will be used to store both national and chapter documents.
- A member may be tasked by the ICT director to maintain the repository.
- The repository should be open such that it can be freely accessed by authorized personnel.

3.7 Document and file naming

The following shall be observed when uploading documents to the repository.

- Avoiding ambiguity

- Avoiding storing open files with sensitive member(s) personal data, if need be the file should be zipped and be password enabled.
- Avoiding uploading the same document multiple times.

3.8 Referencing system.

The following will be the standard guide and file naming system to be followed before uploading any file to the Team's repository.

a. Should contain a Fixed initial-NST at the beginning of the filename-to show its a NUSETA document
b. Followed by a forward slash(/)
c. Followed by Initials for either chapters or the National team e.g. K.U, MOI, and NDF for Ndeffo as agreed by the National executive.
d. Followed by a forward slash(/)
e. Followed by Document type initials e.g. Internal Memo, Budgets, Updates, Minutes etc. as agreed by the National Executive
f. Followed by a forward slash(/)
g. A unique Release series number-Should be incremental e.g. 200,201...
h. Followed by a forward slash(/)
i. Followed by Year of release e.g. 21,20,19

3.9.1 FINAL REFERENCE SAMPLE:

- EXAMPLE ONE: minutes in K.U chapter

  NST/K.U/MNT/200/21

- EXAMPLE TWO: budget released by the National Exec

  NST/NT/BDT/001/21

4 Acceptable Use Policy

4.1Introduction

The purpose of this policy is to provide guidance the National ICT Committee (NICTC) and other users on the acceptable use of our Information and Communication Technology (ICT) equipment and services, and to ensure that these services are used responsibility.

4.2Ownership

All ICT equipment, software and data are the property of NUSETA unless there is an agreement to the contrary.

Examples of our ICT equipment and services include but are not restricted to: desktop computers, laptop computers, network servers, Internet service, keyboards, mice, monitors, telephones, voicemail, video conferencing, mobile telephones, PDA devices, SMART devices, network cabling, network equipment, telephone cabling, power cabling, printers, scanners, fax machines, software, (website, mail domains and SMS domains) electronic file storage, storage devices, tablet devices and storage media.

4.3 Scope

This policy applies to all members of the NICTC and NEB and others who have access to our ICT services.

• The internet and email are easy and often informal ways of communicating. However, expressions of fact, intention and opinion in an email could be binding legally and may be produced as evidence in court. You should therefore take care when using email, blogs or mailing lists as a means of communication. (In short: THINK before you SEND);

• Downloading, copying, possessing and distributing certain material from the internet or by email may be illegal.

• Information relating to members should be treated as confidential and only shared if there is a legitimate reason to do so. Personal information should not be shared

• Users members of NICTC should not use NUSETA systems to store sensitive information for their own personal or non-Team purposes. They are expected use our ICT services to support the work of team and undertake their duties.

4.4 Social Media

Regarding the personal use of social media, the expectation is that users behave professionally in all situations which relate directly or indirectly to the team and should conduct themselves in a way which acknowledges the logical standards of behaviour expected... Users must also exercise their judgement in the use of team's social media platforms – whether or not they explicitly identify themselves with the team on their personal accounts to avoid posting material which may cause the team any reputational damage

4.4.2prohibited use

• Unauthorised downloading of files or applications (e.g. music, movies, games, pornography) on the team's infrastructure.

. • Sending emails or storing information with pornographic, gambling or obscene content.

• Visiting or trying to visit pornographic, gambling or obscene websites or websites promoting violence.

• Revealing passwords to NICTC non-members or other non-relevant personnel.

• Wilful or intentional damage to our ICT infrastructure; introducing password detecting software or any form of computer virus.

• Introducing unauthorised software or hardware to our ICT infrastructure.

A prohibited website and offensive material includes content of a sexually explicit or sexually oriented nature; material that would offend others on the basis of age, disability, gender, marriage and civil partnership, pregnancy and maternity, race.

5. Security

Any system developed should undergo security scrutiny from a different developer other than its designer who is experienced/knowledgeable in the field.

Any system with security loopholes should not be used totally until the loophole is addressed.

5.1Emails

All NICTC are required to comply with the following basic security measures when using email:

- NUSETA has a firewall and spam filter in place but if you are suspicious of an email or an email attachment do not open it and either use the 'report as spam' function or inform the ICT director
- Never send the team's information to your personal email account or anyone else's personal account unless authorised to do so.
- You may send non-team information to your personal account for your personal convenience
- Never send sensitive personal data by email unless encrypted or authorised to do so.

5.2Printing

- Do not leave sensitive or personal data printing unattended.
- Always ensure you take all your printed material with you.
- Always make sure your print was completed successfully and is not simply waiting for consumables, such as paper or toner, or has a paper jam or other technical fault.

Secure disposal: hardcopy and digital. Documents that are no longer needed and that contain personal or Teams information of a sensitive nature should be deposited securely.

5.3Systems security.

- It is the responsibility of NICTC to ensure secure firewalls and appropriate antivirus software is in place and that these are upgraded and maintained regularly. It is also the responsibility of NICTC to ensure that disaster and backup procedures are in place and tested

appropriately. The electronic systems rely on user-IDs and passwords for security, so keeping passwords safe is a critical aspect of effective security.

- The most robust password is alpha-numeric and changed often.
- Do not use your personal email accounts for Teams work. Use the reserved mails for the team

5.3.1Criteria for any teams password:

- • Minimum length of 8 characters.
- • Must contain at least one alpha character, one numeric character, and one special character – for example: £, $, *, @, &, etc.
- • The system will remember your three previous passwords.
- • Passwords should be changed every 60 days minimum.
- • You will be locked out after three incorrect attempts to log on.

• Password changes can be simple alterations of the above by using different symbols or additions to the end or beginning of the password, although it is advisable to completely change your password at least once a year

• If you use multiple systems, then using the same password is acceptable if it is a strong one, but this must be changed regularly.

- Passwords must never be shared with anyone else who is not recommended by the NICTC. this includes other committees, NEB and chapter or cell Executive Committees

5.4Data Security Incident Procedure

Introduction

This section sets out the procedure for handling and reporting a data security incident

Scope

This procedure covers incidents relating to both personal data held on the team's infrastructure, and confidential team information.

- A personal data breach is any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data processed by NUSETA, including data processed on behalf of NUSETA by a third party.
- A data security incident is any incident which is, or risks leading to:

i. A personal data breach, as defined above.
ii. The accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, confidential team information.
iii. Any incident which risks either of the above occurring.

Data security incidents include but are not limited to:

- The loss or theft of data, or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Human error leading to unauthorised disclosure, including verbal disclosure.
- Hacking attacks.
- Accidental deletion of information.

A data security incident could compromise the confidentiality, integrity or availability of NUSETA information. If such an incident should occur then these procedures must be implemented without delay. The focus of any response should be to minimise the impact on NUSETA and any individuals whose data is involved in the incident.

a) NICTC must record all incidents that pose a significant risk to the security of the team's data. This includes incidents that do not result in information being lost.
   By recording these incidents, NICTC is able to identify areas of risk and help prevent breaches in future.

b) Reporting information security incidents should be done to the NEB as soon as they become aware of the issue.

5.4.1 The report should include

i. Date incident occurred
ii. Date incident discovered Incident
iii. Incident reference
iv. Date report completed
v. Incident risk level
vi. Give a summary of what happened.
vii. What data was involved in the incident?
viii. Was personal information involved in the incident?
ix. Was special category information involved in the incident?
x. Was sensitive information involved in the incident?

- Regarding a data breach. Careful consideration should be given regarding any notification message. It is vital that we understand the details of the breach and are able to provide useful information. However, it is also vital that we respond in a timeous manner
- You should consider including the following:

i. Details of what happened and when the breach occurred.
ii. What data was involved?
iii. What steps have been taken to contain the breach and prevent reoccurrence?
iv. Advice on what steps to take, e.g. contact banks.
v. How you will help and keep them informed.
vi. Provide a way to be contacted.