

## 1. **Introduction and Purpose**

- 1.1 Information security is concerned with the safe keeping of information, in electronic and paper format. The main purpose of implementing good information security is to allow the effective and efficient use of information. Further, it is the safeguarding of the organisation's (Novena University) data from unauthorised access or modification, and to ensure data availability, confidentiality, and integrity to all.
- 1.2 This policy is a key component of Novena University's overall approach to information governance and should be considered alongside all other information governance and cybersecurity policies.
- 1.3 The main aim of this policy is to advise staff, students, and other organisations dealing with the university of their obligations with regards to confidentiality and where to seek further guidance and assistance. The objectives of this policy are to preserve information according to the following categories:
- **Confidentiality** – Access to the university's data shall be confined to those with appropriate authorization.
  - **Integrity** – Information shall be complete and accurate. All systems, assets, and networks shall operate correctly, according to specifications in the university brief.
  - **Availability** – Information shall be available and delivered to the right person, at the time when it is needed.

## 2. **Scope**

- 2.1 This policy applies to:
- Novena University as an institution;
  - All subsidiary entities of Novena University;
  - All staff of Novena University and its subsidiary companies;
  - Everyone (including contractors and suppliers etc.) working for or on behalf of Novena University or its subsidiary companies.
- 2.2 This policy also applies to all data that Novena University holds.

## 3. **Definitions**

- 3.1 **System Level Security Policies (SLSPs)** – Documentation specific to a system or systems, covering security and management procedures in place to ensure the security of the system.
- 3.2 **Information Security Management System (ISMS)** – The governing principle behind the ISMS is that an organisation should design, implement, and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk to Novena University and subsidiary companies.
- 3.3 **Information Asset** – Information held which is of value to Novena University. This is generally a body of records or information managed as a single entity.

3.4 **Information Security Incident** – is any incident which affects the confidentiality, integrity or availability of any information of value to Novena University.

#### 4. **Roles and Responsibilities**

4.1 Everyone who works for or with the Novena University and its subsidiary companies has some responsibility for ensuring data is collected, stored and handled appropriately ensuring its security based on the policy herein.

4.2 The **Board of Council** is ultimately responsible for ensuring that the Novena University and its subsidiary companies meets its legal obligations as it concerns their dealings with the University.

4.3 Overall responsibility for this policy lies with the University's Chairman of the University **Vice Chancellor** who will be a member of the University's Management Staff.

4.4 As part of his responsibilities, the university's **Data Protection Officer** is responsible for drawing up all information governance policies, including data protection and information security policy.

4.5 **The Cyber Security Officer alongside the Data Protection Officer** are responsible for developing IT security policy, standards and guidelines. These two officers are also responsible for ensuring that effective IT security systems are operationally implemented, fit for purpose and available across the University.

4.6 **All Faculty Provosts and Heads of Departments** have the responsibility for ensuring compliance with information governance policies within their areas of responsibility, and will assume the role of **Director of Information and Communication Technology (otherwise known as Information Asset Owner)** within their areas of responsibility. The Director ICT will assign information asset administrator(s) from their areas of responsibility.

#### 5. **Policy Details**

5.1 All information handled by the University is handled in line with all applicable laws and regulations as stated in the Nigerian Universities Commission's guidelines documentation.

5.2 All relevant University records and information will be classified, in line with the Novena University Brief Document.

5.3 All records and information are organised into groups known as Information Assets where it is appropriate to do so in line with the University Guideline Document (University Brief).

5.4 All Information assets will be risk assessed in line with the Information Risk Management processes and procedures. The outcome of each risk assessment will be shared and where necessary, appropriately acted upon by the University Management Committee.

5.5 All access to information assets is usually controlled by the appropriate asset owner / administrator (Provost and HOD) ensuring a minimum required access model is followed. Our information access is periodically (**mostly bi-annually**) reviewed and amended as applicable.

- 5.6 All information security incidents are centrally reported, and where applicable, remedial recommendations are made and followed up. Reporting of information security incidents is usually carried out in line with the Information Security Incident reporting procedure.
- 5.7 Information Asset Owners shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.
- 5.8 Where information is being shared, stored or processed outside of the university controlled environment, sufficient assessment is usually carried out on the recipient to ensure the security of university data. All data sharing activity is covered by appropriate data sharing agreements or other contractual clauses.
- 5.9 All technical security measures, will be taken where appropriate so to protect information. Details of technical security measures can be found in the IT Security Policy and associated documentation.
- 6. **Training.**
- 6.1 All staff are trained as part of their Information, Cyber Security and Data Protection Training in line with Management's vision for information protection needs of the university.
- 6.2 All Provosts and HoDs of our university do receive additional training above and beyond the basic staff training. This is delivered face to face by a member of the Information Governance Team.
- 6.3 This policy is periodically reviewed and uploaded to our online repository with all staff prompted to review the policy. An analysis of staff uptake is monitored, with follow-up communications issued as necessary.
- 6.4 This policy is also uploaded to our university website along with all associated processes, procedures and guidance notes.