Policy Statement: The aim of this policy is to establish guidelines and procedures for the appropriate and secure use of Institution email accounts, to ensure the confidentiality, integrity, and availability of email communications while promoting professional conduct, compliance with legal and regulatory requirements, and protection against unauthorized access and data breaches. This policy applies to everyone who is provided email services, such as University and visiting faculties, staff, students, contractors, consultants and guests ("users").

1. Purpose: The purpose of this policy is to define the rules and guidelines for the usage of institution email services. It outlines the responsibilities and expectations of users regarding email communications to maintain a secure and professional communication environment.

2. Scope: This policy applies to all University and visiting faculties, staff, students, contractors, consultants and authorized users ("users") who have been provided with institution email accounts. It covers all email communications sent, received, or accessed through institution-provided email systems and platforms.

3. Email information:
   - 3.1. The student mailbox storage size is 15 GB.
   - 3.2. The syntax of the email address is the initial of the first name, followed by the last name, followed by the last three digits of the student id #. For example, the email address of the student John Doe, ID 123456, is jdoe456@students.auf-florence.org.
   - 3.3. One year after graduation, the student ID will be deactivated and the mailbox (and all content) will be deleted.

4. Policy Guidelines:
   - 4.1. Authorized Use:
     - 4.1.1. Institution email accounts are provided to allow users to perform all the tasks related to the University activities .
     - 4.1.2. Institution uses two kinds of mailboxes: service mailboxes and user mailboxes. Service mailboxes manage emails related to AUF services. Access to these mailboxes is granted by delegation to staff members in charge of these services.

4.1.3. Users are responsible for the content and accuracy of their email communications and should exercise professionalism, ethical behavior, and compliance with all applicable laws and regulations.

4.1.4. The standard method to access Institution mailboxes is by web browser or iOS/Android app. Further access protocols are IMAPS or POP3S, although their use is discouraged.

4.1.5. Institution mailboxes are working tools and as such they and their content are owned by the Institution, which retains the right to access them. Institution permits the use of these mailboxes for personal emails but users should be aware that personal material in the mailbox and related services (Google Drive, Google Docs, Google Sheets, etc.) can be viewed by AUF in any investigation and, as such, shall have no expectation of privacy in anything they store, send or receive on the Institution email system.

4.2. Account Security:

4.2.1. Users must protect their institution email accounts and associated credentials (username and password) from unauthorized access.

4.2.2. Users should never share their institution email account credentials with others or use another person's email account to send or receive emails.

4.2.3. Users must comply with password complexity requirements, change their passwords periodically, and refrain from using easily guessable or commonly used passwords.

4.2.4. If there is suspicion of a compromised email account or unauthorized access, users must immediately report the incident to the IT department.

4.3. Email Content and Usage:

4.3.1. Users should exercise caution when composing emails to ensure that the content is professional, appropriate, and relevant to work-related matters.

4.3.2. Users must not send or forward unsolicited commercial emails (spam) or any form of unauthorized bulk emails from their institution email accounts.

4.3.3. Users should refrain from sending any disruptive, discriminatory, harassing, offensive or intimidating messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

4.3.4. Users must not transmit confidential or sensitive information through email unless it is appropriately encrypted or protected according to organizational guidelines.

4.3.5. Users should be aware that email communications may be monitored or audited for compliance with this policy, legal requirements, or as part of investigation procedures.

4.4. Email Attachments and Links:

4.4.1. Users must exercise caution when opening email attachments or clicking on links, especially if they are from unknown or suspicious sources.

4.4.2. Users should use up-to-date antivirus software and perform regular scans on attachments before opening them to mitigate the risk of malware infections.

4.5. Email Retention and Archiving:

4.5.1. Users should regularly review and manage their email storage, deleting unnecessary emails.

Non-Compliance: Failure to comply with this policy may result in disciplinary action, up to and including termination of the relationship between the user and the Institution, as well as legal consequences if applicable.

Policy Review: This policy will be reviewed on an annual basis or as deemed necessary by the institution's management to ensure its relevance and effectiveness.