**Lipscomb Email Security Policy**

**By: Jonny Hughes and Keaton Sample**

**1 Overview**

Email is a main method of communication within the business environment between customers, employees, and even between companies. Thus it is severely important to be well educated and aware of the safety risks which are associated with using email. In this Policy we will lay out a framework on how to avoid scams, viruses, phishing, and other sorts of malicious attempts to steal information or infiltrate a network.

**2 Purpose**

The purpose of this email policy is to ensure the proper use of Lipscomb email system and make users aware of what Lipscomb deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within Lipscomb Network.

**3 Scope**

This policy covers appropriate use of any email sent from a Lipscomb email address and applies to all employees, students, and other members of the community operating on behalf of Lipscomb.

**4 Policy**

4.1 All use of email must be consistent with Lipscomb policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

4.2 Lipscomb email account should be used primarily for Lipscomb school or business related purposes; personal communication is permitted on a limited basis, but non-Lipscomb related commercial uses are prohibited.

4.3 All Lipscomb data contained within an email message or an attachment must be secured according to the Data Protection Standard.

4.4 The Lipscomb email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Lipscomb employee or student should report the matter to their supervisor immediately.

4.5 Sending chain letters or joke emails from a Lipscomb email account is prohibited.

4.6 Lipscomb employees shall have no expectation of privacy in anything they store, send or receive on the company’s email system.

4.7 Lipscomb may monitor messages without prior notice. Lipscomb is not obliged to monitor email messages.

4.8 Do not click on a link without first verifying the reliability of the source the link has been provided from. If you are unsure of the status of the source, hover over said link to ensure the link is sending you to the exact webpage you are expecting.

4.9 Reliability of a Source can be checked by examining the Grammar of the email, as phishing emails have not been through a business approval check. Another source check is to ensure the email address the link or information is coming from, to see if it is a Lipscomb associated email, or another trusted source. Also check the header of the email to ensure it is specific to you, as generic emails are sent out in mass by scammers without applying information to specific users.

4.10 If you do click a link which has taken you somewhere strange, triggered a download onto you device, or some other unusual and unexpected action has occurred, immediately notify Dr. Simmons, and let him know that there may be a security risk. This allows him to deal with the issues as quickly as possible.

**5 Policy Compliance**

5.1 Compliance Measurement

- Dr Simmons himself will find out about what was done and apply the appropriate punishment.

5.2 Exceptions

- Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

- An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or being expelled from the University.

**6 Definitions and Terms**

**7 Revision History**

Updated For Info Sec