

E-mail Security and Privacy Policy

Purpose

This policy statement provides specific instructions on the ways to secure electronic mail (e-mail) resident on personal computers and servers.

Security

No Encryption - All e-mail processed via UMHB's mail servers are not encrypted. If sensitive information must be sent by e-mail, encryption or similar technologies to protect the data must be employed.

Message forwarding - Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, e-mail users should exercise caution when forwarding messages. Sensitive information must not be forwarded to any party outside the University without the prior approval of the department chairperson and/or vice president. Mass forwarding or broadcasting of messages to recipients outside University of Mary Hardin-Baylor is prohibited unless the prior permission of the Vice-President has been obtained.

Falsifying e-mail - It is relatively easy to forge another user's e-mail. Likewise, e-mail received from an unknown source should not be trusted unless a due diligence process has first been performed.

Privacy

Respecting privacy rights - Employees may not intercept or disclose, or assist in intercepting or disclosing electronic communications except as otherwise specifically provided. UMHB respects the rights of its employees and students, including their reasonable expectation of privacy.

No guaranteed message privacy - UMHB cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications, depending on the technology, may be forwarded, intercepted, printed and stored by other unauthorized users. Further, in case of a request from law enforcement authorities or university official, your e-mail and other data may be made available to the requesting agency.

Regular message monitoring - UMHB does not regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support investigation of policy violation activities. Users should structure their electronic communications in recognition of the fact that UMHB reserves the right to examine the content of electronic communications.

Statistical data - Consistent with generally accepted business practice, the Information Technology Department collects statistical data about electronic communications. Using such information, Information Technology staff monitors the usage of electronic communications to ensure the ongoing availability and reliability of these systems.

Incidental disclosure - It may be necessary for IT staff to review the content of an individual employee's communications during the course of problem resolution. IT staff may not review the content of an individual employee's communications out of personal curiosity or at the request of individuals who have not gone through proper approval channels.