

3.20 USE OF TECHNOLOGY AND EQUIPMENT**3.20.1 INTENT:**

To ensure safe and appropriate use of equipment, the Internet, systems, and networks, as well as transparency of monitoring by LICA.

3.20.2 DIRECTIVES:

- Employees will be provided with all the equipment necessary to fulfill job assignments, including computers and communication devices. The allocation of such equipment will be approved by the Board.
- Employees must abide by the procedures set out in this policy to ensure the safe, appropriate, and legal use of LICA equipment.
- LICA will require Employees to be trained in the use of technology. Training, at a minimum, will be completed through internal team review and may be provided externally as approved by the Board of Directors.

3.20.3 SCOPE: All Employees, Contractors, Board of Directors, Committee Members, Volunteers.

3.20.4 IMPLEMENTATION:**3.20.4.1 USE OF THE ONE DRIVE & LICA SERVER:**

- The One Drive and SharePoint are for business use only.
- LICA Employees are prohibited from downloading any files from the One Drive and/or SharePoint onto personally owned equipment.
- If an Employee creates, stores, or transmits LICA business information onto personally owned property (including, but not limited to, laptop computers, desktop computers, cell phones, memory cards, or printed paper, etc.), the business information remains the expressed property of LICA.
- Approval is required prior to copying, destroying, or altering any data, documentation, or other information that belongs to LICA.

3.20.4.2 INTERNET ACCOUNTS / APPLICATIONS:

- LICA Internet accounts and applications are to be accessed only by assigned users for legitimate business purposes only.

Review Dates: May 8, 2024
Approval Dates: May 23, 2024

- Employees are authorized to use personally owned equipment or property to access LICA business information where direct access is provided, such as a personal mobile device to access LICA information on applications and SharePoint.
- All LICA information and correspondence, including email, transmitted or received using our computer-based technology, is the business property of LICA and is to be managed accordingly for appropriate business-related matters.
- Employees are not authorized to share or distribute any LICA information and correspondence received through their accounts unless otherwise approved.
- As LICA computers and network files are not private, it is recommended that personal files are not stored on them.

3.20.4.3 PASSWORD PROTECTION:

- Internet access at LICA is managed via a private account and password.
- LICA's security system is managed via individual user passwords that must remain confidential.
- All usernames and passwords for LICA-owned and operated devices must be supplied to Management.
- If an Employee terminates employment with LICA for any reason, Management will remove the former Employee's access to the LICA email, security system, and other applications.

3.20.4.4 SECURITY:

- Passwords must be protected (e.g., not written down in an obvious location, not saved to a shared device, etc.).
- Passwords are not permitted to be disclosed to or shared with other users or third parties.
- If an Employee has reason to believe that their password has been compromised, they must update their password.
- Employees are not permitted to engage in any activity that could compromise the security of LICA host servers, computers, or devices.
- Employees are not to open any unverified links or attachments from any unknown email addresses (always check the full email address not just the username). Suspicious emails are to be forwarded to IT for verification prior to downloading or opening any links/attachments.
- Employees who travel are not to leave LICA computers or devices unattended in their vehicles.

Review Dates: May 8, 2024

Approval Dates: May 23, 2024

3.20.4.5 INTERNET USE GUIDELINES:

- Internet use must align with all LICA policies, including ethical and legal conduct.
- Employees are not authorized to stream videos or music while on LICA internet or Wi-Fi, which hinders network performance.
- Non-work-related data (including video and sound files) must not be downloaded from the Internet unless their use has been authorized for the purposes of conducting LICA business.
- Employees must refrain from online practices or procedures that expose the network or resources to virus attacks, spyware, adware, malware, or hackers.
- Employees are responsible for familiarizing themselves with procedures for downloading and protecting information in a secure manner, as well as for identifying and avoiding any online material deemed sensitive, private, confidential, and copyrighted.
- Employees utilizing the Internet must always conduct themselves in a professional manner.
- Employees must not disclose confidential LICA information or intellectual capital to unauthorized third parties.
- Internet is provided for work use; Employees may use it for incidental personal use provided that such use does not conflict with any LICA policy. LICA may revoke this privilege at any time.
- LICA does not accept responsibility for any loss or damage suffered by Employees because of Employees using LICA's Internet connection for personal use.

3.20.4.6 EMAIL:

- LICA's email communications must be conducted with respect to the standards of conduct and should be created with professionalism and attention to detail.

3.20.4.7 ACCESSING AND MONITORING USAGE RECORDS:

- LICA reserves the right to monitor any activity on its hardware, Internet usage, software, LICA emails, LICA applications, equipment, and LICA accounts.
- Use of LICA's Internet resources implies the user's consent to web monitoring for security purposes.
- While individual usage is not routinely monitored, unusual or high-volume activities may warrant more detailed examination as determined by Management.
- Only the Executive Director or Board Officers may examine such usage/records for business-related issues for investigation to determine misconduct, as directed by the Board of Directors.

Review Dates: May 8, 2024

Approval Dates: May 23, 2024

- LICA will do its best to accommodate Employee privacy while being diligent and thorough when conducting investigations regarding LICA’s email and Internet usage.

3.20.5 USE OF LICA EQUIPMENT:

- The LICA-supplied equipment is intended for their assigned LICA purposes only.
- LICA strictly prohibits the use of LICA-provided equipment for conducting unapproved activities, such as alternate sources of employment or home-based businesses, whether compensated or not.
- If an Employee is required to use any LICA-supplied equipment for reasonable non-work-related reasons, the Employee must obtain management authorization prior to using the equipment. The use must meet the acceptable guidelines in this policy, and it must be done on the Employee’s own time.
- From time to time, LICA may update equipment and property and adopt sustainable technologies to ensure efficiency and sustainability. This may include efficiency for impacts on Employees, LICA, and the environment.

3.20.6 MAINTENANCE/CARE:

- Employees are responsible for safeguarding any equipment assigned to them and ensuring that the equipment is maintained correctly.
- An Equipment User Agreement Form must be signed before an Employee receives LICA equipment.
- Employees are expected to adhere to all operating instructions and guidelines, safety standards and general care instructions when operating LICA equipment.
- If LICA materials or property are lost, stolen, or damaged, the Employees are required to report the loss or incident to their Reporting Manager as soon as possible and will be required to participate in any investigations deemed necessary, whether or not it is a viable piece of equipment.
- Damaged equipment or materials should be returned to their Reporting Manager for assessment, repair, or warranty service.
- Employees are required to safely store equipment that is not in use to minimize any possible damage.

3.20.7 SUPPORTING DOCUMENTS:

- Equipment User Agreement Form

Review Dates: May 8, 2024

Approval Dates: May 23, 2024
