LANDRY'S®

DINING · HOSPITALITY · ENTERTAINMENT · GAMING

Security Awareness Training

Physical Security

Device, Web & Email Security

Password Security

Social Engineering

Reporting

Physical Security Awareness

It is important to protect your property and premises against, theft, crime, and unauthorized personnel attacks.

- Do not let anyone piggyback/tailgate you through a badge-restricted area
- Always lock your workstation when you step away from your desk
- Shred documents with sensitive information or place them in a secured shredder collection box

Physical Security Awareness

It is important to protect your property and premises against, theft, crime, and unauthorized personnel attacks.

- Always secure your belongings and valuables
- If you see anyone loitering/trespassing or attempting to access an unauthorized area, alert your supervisor immediately
- If you encounter a situation that poses a threat to anyone's life or safety, immediately dial 911 and follow up with your supervisor afterward as soon as possible

Device, Web & Email Security

Exercise caution and discretion online:

- Scrutinize URLs and attachments carefully
- Avoid websites that host illegal/malicious/lascivious content
- Ensure HTTPS is enabled on websites before entering passwords or secure information
- Use a secure, up-to-date browser ex: Talon
- Do not perform any sensitive tasks on public Wi-Fi (unless connected to VPN)

Device, Web & Email Security

Exercise caution and discretion online:

- Never use USBs on company-issued devices without prior authorization from IT Security
- For personal devices (smartphones, tablets, laptops): check periodically whether apps and OS are up-to-date; install available patches and updates promptly
- Report unexpected or unusual device activities (e.g., screens turning on/off by themselves; sudden performance drop) to IT Help Desk
- Never give someone else access to your company email, work-related accounts, or company-issued devices without explicit permission from IT Security
- Adhere to all Information Technology guidelines as outlined in the Employee Handbook

LANDRY'S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

COMPUTER TECHNOLOGY

PERSONAL ELECTRONIC DEVICES

CLOUD BASED STORAGE

E-MAIL/INTERNET SYSTEMS

ELECTRONIC MONITORING

COMPUTER TECHNOLOGY

The Company’s computers, systems and employee communications network are some of the most important assets because: (1) they are critical to the accuracy and proper control of financial transactions in the Corporate Office; and (2) they represent a large investment by the Company in software and hardware.

Therefore, all employees are responsible for assisting in the care of Company computers and Company issued electronic devices as defined in the following basic procedures:

- Company personnel must seek diligently to protect all computer hardware and Company issued electronic devices from elements of physical abuse, including exposure to harmful substances (liquids, food, etc.) and all forms of carelessness/misuse.
- All questions/problems concerning the computer hardware, software or network should be communicated by appropriate Company personnel to the Technology Support Center (TSC). TSC support is available seven days per week, 24 hours per day. All calls to thirdparty service providers (hardware vendors, and/or local service providers) must be arranged by TSC representatives.
- Under no circumstances are Company personnel permitted to arrange third-party services without the direct involvement of the TSC.

LANDRY’S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

COMPUTER TECHNOLOGY (continued)

- The computers installed are customized systems that are designed and configured for specific business purposes and are the property of the Company. Therefore, under no circumstances are company computers or other electronic devices to be used for any private, non-business purpose.

- System security and integrity is of vital importance in safeguarding the Company's information and assets. Therefore, it is incumbent for each employee to observe the basic rules of security:

- Employee security passwords are confidential and must never be shared between employees.

- Absolutely no new software or new version of a currently-installed software product is to be installed on any Company computer or Company issued electronic device without the approval and direct involvement of the TSC (unauthorized software includes all games, screen savers, wallpapers, all Internet browsers and all other software products/versions that are not specifically approved for installation).

- Absolutely no change to the hardware, wiring/cabling or component configuration is permitted without the approval and direct involvement of the TSC.

LANDRY'S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

COMPUTER TECHNOLOGY (continued)

- Storing work data on physical devices, including but not limited to USB drives, memory cards, or external hard drives, must be pre-approved by the IT Department. Employees must only use such storage devices provided by the Company, and should never use or plug in a storage device that is found or has been given as a promotional item, as these devices may contain hidden malware or viruses.

- Lost or stolen storage devices must be reported to the IT Department and your Department Manager immediately to help ensure their safe return and/or prevent a potential data breach.

- Work data or information must never be shared over unauthorized email accounts, social media accounts such as Facebook, LinkedIn, Instagram, Snapchat, etc., or through text messages (unless such text message is on a Company approved phone or other device).

- To prevent a data breach, the following types of information must be encrypted by a strong password before dissemination: Personally Identifiable Information (Social Security Numbers, medical information, passport number, driver's license number, biometric information/fingerprints, photographic/facial images, vehicle registration numbers, taxpayer information), financial data (bank account, credit/debit cards), and sensitive Human Resources data (pay rates, disciplinary documentation). Such data should never be copied, forwarded or otherwise made available to anyone outside of the encryption process.

LANDRY'S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

COMPUTER TECHNOLOGY (continued)

- All Company-issued and approved electronic devices (mobile phones, desktop computers, tablets, etc.) must be secured in a “locked” mode when not in use by the employee to prevent unauthorized access to the Company’s information systems and data. For Company-approved mobile phones and tablets, you must set a password or you may use the biometric recognition feature in order to unlock the device.

LANDRY'S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

COMPUTER TECHNOLOGY

PERSONAL ELECTRONIC DEVICES

CLOUD BASED STORAGE

E-MAIL/INTERNET SYSTEMS

ELECTRONIC MONITORING

PERSONAL ELECTRONIC DEVICES

This policy, referred to as Bring Your Own Device (BYOD), establishes guidelines for eligible employees' use of personally owned electronic devices to access Company systems, services and data. Regardless of the foregoing, personal devices are not permitted to be used for any personal reasons while working. Failure to follow Company policies and procedures may result in disciplinary action, up to and including termination of employment.

The Company does not provide electronic devices, including cellphones and/or tablets. In addition, all expenses associated with a personally owned device, including but not limited to WIFI access, accessories, charging cords, device repair and service overages are the employee's responsibility. Certain qualified employees who are required to stay connected in order to provide support during non-business hours may be eligible for a monthly allowance. Qualified employees will be notified by their supervisor. Employees who do not have written authorization from their supervisor to utilize their personal device to access Company systems are not entitled to reimbursement.

Eligible employees may use the carrier of their choice. The company maintains relationships with AT&T, Verizon, and Sprint, which gives all employees access to discounts on equipment and service. Information on discounts provided by these carriers is located on the Employee Portal.

LANDRY'S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

PERSONAL ELECTRONIC DEVICES (continued)

Employees are never required to download or utilize applications for work purposes on their personal phones. However, should you choose to use an application as a resource, please remember that you can use the wifi at your work location to access the applications.

Employee’s Responsibilities:

- Use the device’s security features, such as a Biometric, PIN, Password/Passphrase and must set the device to automatically lock if idle for 5 minutes.

- Install and configure tracking and/or wiping services, such as Apple’s ‘Find My iPhone app’, Androids ‘Where’s My Droid’ or Windows ‘Find My Phone’, where the device has this feature.

- Remove all company information from the device and return it to the manufacturers’ settings before selling, exchanging or disposing of a device.

- Report to the IT Helpdesk immediately in the event that your device is lost or stolen or its security is compromised, so that the device can be remotely “wiped” of all company data.

- Only connect electronic devices to secure WIFI connections.

- Use of a rooted (Android) or jailbroken (IOS) device to access the company network is not permitted.

LANDRY’S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

PERSONAL ELECTRONIC DEVICES (continued)

- Employees are never required to download or utilize applications for work purposes on their personal phones.
- Keep devices up-to-date with manufacturer or network provided patches.
- Texting or emailing while driving is strictly prohibited.

No employee communication made using the company's systems is considered private or confidential and employees should have no expectation of privacy with respect to any use of the company's systems. We reserve the right, at any time, for any reason, and without notice to or consent of users, to access all information conveyed or stored anywhere on any of our electronic systems, including telephone calls and electronic mail messages, even if the information has been password protected or encrypted. We may use the information so obtained for any legal purpose including disclosure to third parties, subject only to applicable law, but otherwise in our sole discretion. We may exercise this right in the course of an investigation or as we deem necessary to locate substantive information that is not more readily available by some other less intrusive means. We may disclose the contents of any electronic communication sent to or received by any employee and may use information regarding the number, sender, recipient and address of messages sent over the electronic mail system for any purpose.

LANDRY'S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

COMPUTER TECHNOLOGY

PERSONAL ELECTRONIC DEVICES

CLOUD BASED STORAGE

E-MAIL/INTERNET SYSTEMS

ELECTRONIC MONITORING

CLOUD BASED STORAGE

The Company assigns cloud-based storage accounts to certain approved employees to store and securely share files as necessary with other employees. Only Company approved and assigned cloud-based storage accounts may be utilized. If an employee requires access to documents and files outside of work, they must obtain an approved account from the IT Department. The use of the Company’s cloud-based storage accounts is reserved solely for the conduct of business at the Company and may not be used for personal business or any other purpose.

- All documents created, stored or shared in a Company cloud-based storage account are the property of the Company.
- Documents in a Company cloud-based storage account may never be shared or distributed to anyone outside of the Company.
- If you have a personal Dropbox or other cloud based storage account, you may not transfer Company documents into your personal account.
- Employees may not move Company documents out of a cloud-based storage account without permission of the document owner or the IT Department.
- You may only share documents relevant to employees with whom you share a cloud-based storage account. Never assume that others should have access to confidential information.

LANDRY’S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

CLOUD BASED STORAGE (continued)

All Company cloud-based storage accounts will be monitored and documents saved in and removed from the accounts will be monitored. Violation of this policy may lead to disciplinary action up to and including termination of employment.

LANDRY'S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

LANDRY'S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

COMPUTER TECHNOLOGY

PERSONAL ELECTRONIC DEVICES

CLOUD BASED STORAGE

E-MAIL/INTERNET SYSTEMS

ELECTRONIC MONITORING

E-MAIL/INTERNET SYSTEMS

The use of the Company’s electronic mail (“e-mail”) and Internet systems is reserved solely for the conduct of business at the Company. It may not be used for personal business or any other purpose.

All messages created, sent or retrieved over the e-mail and Internet systems are the property of the Company and should be considered public information. The Company’s senior management reserves the right to access and monitor all messages and files on the computer system as deemed necessary and appropriate.

It is important that all employees maintain a professional demeanor when communicating via the Company’s e-mail system. Company e-mail is not to be used as a forum to express your nonbusiness related beliefs or agendas. Your signature line should include your contact information only (name, title, phone number, email address, etc.), and should not include quotes, directives or clip art and should not be used to express your personal causes.

The e-mail and Internet systems shall not be used to send or receive copyrighted materials, trade secrets, proprietary financial information or similar materials without prior authorization from the Company’s management, including forwarding Company emails to your own personal email account. Employees, if uncertain about whether certain information is copyrighted, proprietary or otherwise inappropriate for transfer, should resolve all doubts in favor of not transferring the information and consult the Company’s General Counsel or the Human Resources Department. It is important that employees consider this policy when composing, forwarding, or responding to emails.

LANDRY’S®
DINING • HOSPITALITY • ENTERTAINMENT • GAMING

E-MAIL/INTERNET SYSTEMS (continued)

Confidential business information may inadvertently be disclosed to outside parties by carelessly forwarding an email or by “replying to all” without reading the entire email chain. Always scroll to the bottom of an email and read the entire chain so that you know the entire content before forwarding to anyone inside or outside the Company.

In addition, communications with Company attorneys are privileged and highly confidential, meaning they may be protected from disclosure during litigation. However, this protection may be lost when the communication is forwarded or copied to third parties whether inside or outside the Company. Never forward an email between yourself and a Company attorney to anyone without express written permission and instruction from the attorney.

Use of the e-mail and Internet systems to engage in any communications that are in violation of Company policies is strictly prohibited. The e-mail and Internet systems are not to be used to create or disseminate any offensive or disruptive messages. Among those that are considered offensive are any messages which contain sexual and/or pornographic implications, racial slurs, gender specific comments or any other comments that offensively address someone’s age, sexual orientation, religious or political beliefs, national origin or disability. The e-mail and Internet systems should not be used to disseminate jokes, promote chain letters or other similar types of activities. The e-mail and Internet systems should not be used to disseminate, solicit, promote, encourage, or advertise commercial ventures, religious or political causes, outside organizations, or other non-job related information or solicitations.

E-MAIL/INTERNET SYSTEMS (continued)

To ensure that employees comply with this policy, the Company may conduct periodic audits of, including, but not limited to individual personal computers, disks, or backup tapes if necessary, the Company will advise appropriate legal officials of any illegal violations.

LANDRY'S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

COMPUTER TECHNOLOGY

PERSONAL ELECTRONIC DEVICES

CLOUD BASED STORAGE

E-MAIL/INTERNET SYSTEMS

ELECTRONIC MONITORING

ELECTRONIC MONITORING

In accordance with applicable Federal and State law, the Company may use various monitoring devices at our businesses such as cameras (both inside and outside the property, excluding restrooms) and telephone recording devices which may record conversations or other audio interactions. Such monitoring devices assist us with security and safety as well as for use with training to improve guest service and quality assurance. In addition to the above, occasionally we may videotape and/or photograph our staff members for internal/external promotions and/or request that third parties record interactions with our employees for promotional and/or training purposes.

Generally, access to recordings is limited to individuals with need to review such items. However, when recordings are made for external promotional purposes, the Company's Use of Likeness policy will apply.

Telephone recordings may be used for training purposes and your supervisor may review calls with you to help improve guest relations. Personal phone calls should be made on personal cell phones during breaks in accordance with the Company's Electronic Devices policy.

Employees are strictly prohibited from interfering with the operation of the telephone or video monitoring systems. Any employee found to tamper with the systems or otherwise to have violated this policy will be subject to immediate discipline, up to and including termination. Your acknowledgment of this handbook evidences that you have consented to the monitoring practices of the Company as stated herein.

LANDRY'S®

DINING • HOSPITALITY • ENTERTAINMENT • GAMING

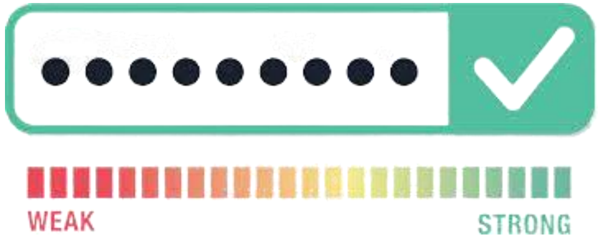
Password Security

Keep passwords private, unique, and secure. Good passwords are usually long and complex. Monitor accounts for signs of suspicious activity.

When creating strong passwords use the following parameters:

- **Minimum** 7 characters

  *However, IT Security **strongly recommends** using a longer password length wherever and whenever possible
- Combine **upper-case and lower-case** letters
- Use special characters such as !@_ when allowed
- Use numbers when allowed

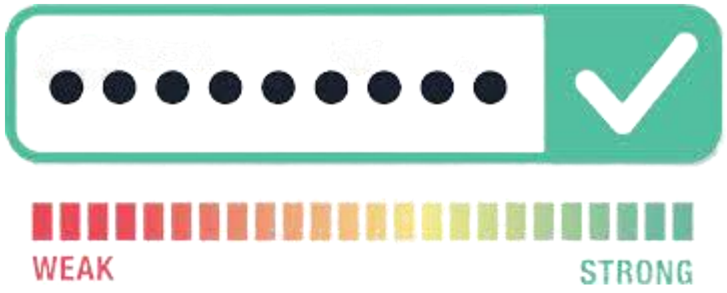


Password Security

Keep passwords private, unique, and secure. Good passwords are usually long and complex. Monitor accounts for signs of suspicious activity.

When creating a password, you should **never:**

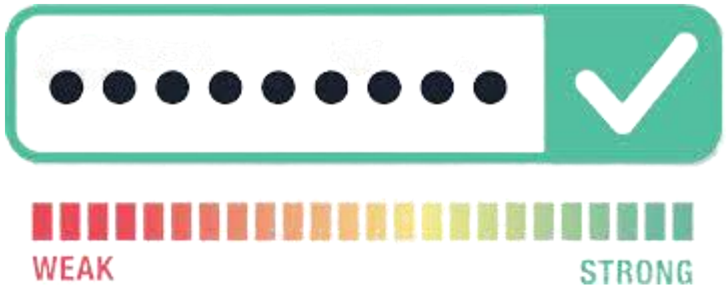
- Use same passwords across multiple sites
- Use easy to guess passwords
- Use only words or names without numbers and special characters



Password Security

Keep passwords private, unique, and secure. Good passwords are usually long and complex. Monitor accounts for signs of suspicious activity.

- Do not write down passwords or expose them to plain view
- Do not store passwords in unencrypted files (ex: Word or Excel)
- Use a password manager such as BitWarden or 1Password
- Set up two-factor or multifactor authentication for all accounts when possible
- Immediately revise compromised passwords



Social Engineering Awareness

Social engineering is any attempt, phone, email, or in person, to deceive, manipulate, or even blackmail or threaten you into doing or sharing something you shouldn’t.

Recognizing Signs of Social Engineering:

- Message arrives unexpectedly
- Sender asks something out of the ordinary
- Requested action is potentially harmful to safety or security
- Attacker attaches an unusual file or URL
- Attacker includes a sense of urgency

Social Engineering Awareness

Social engineering is any attempt, phone, email, or in person, to deceive, manipulate, or even blackmail or threaten you into doing or sharing something you shouldn’t.

Types of Social Engineering Attacks:

- **Phishing-** The use of shortened links or attachments to redirect users with the intent to obtain personal information or install malware
- **Pretexting-**The attacker fabricates a scenario to steal personal information
- **Vishing-** Phishing attacks over the phone to retrieve personal or confidential information
- **Smishing-** Phishing attacks over SMS text messages
- **Quid Pro Quo-** Attackers promise a form of service in an attempt to steal information
- **Tailgating-** Attackers follow employees into restricted areas

Social Engineering Awareness

Social engineering is any attempt made by, phone, email, or in person, to deceive, manipulate, or even blackmail or threaten you into doing or sharing something you shouldn’t.

Recognize Email Phishing:

- Check sender name
- Check sender address for spoofing
- Check recipients (ex: generic, BCC email)
- Scrutinize the subject line and contents
- Exercise caution and discretion with attachments, URLs and requests to disclose sensitive information
- Be vigilant when corresponding with unfamiliar or unrecognized senders

Social Engineering Awareness

Social engineering is any attempt made by, phone, email, or in person, to deceive, manipulate, or even blackmail or threaten you into doing or sharing something you shouldn’t.

Recognize Voice Phishing (vishing) & SMS Phishing (smishing):

- Check and lookup caller ID- phone numbers can easily be spoofed
- Be wary of requests to disclose sensitive information
- Be aware of any requests to send money or make purchases
- When possible, verify the identity of the caller

Reporting

Always assume “Better safe than sorry”. If you see something, say something.

- **Report** suspected credit card, debit card, or bank account fraud to **IT Credit**
- **Report** suspected phishing, malware, and spam to **IT Security**
- **Report** breached or compromised accounts to **IT Help Desk & IT Security**
- **Report** lost or stolen employee ID cards and other company-issued property to **Human Resources**
- **Report** inappropriate, illegal, and suspicious conduct to your **Supervisor**
- **Report** life-threatening emergencies to **911** and follow up with your **Supervisor**