PASSWORD POLICY

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all staffs who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any LUX* Resorts & Hotels site or has access to LUX* Resorts & Hotels network.

General Password Construction Guidelines

Strong passwords have the following characteristics

1. Contain at least three of the five following character classes:
    - Lower case characters
    - Upper case characters
    - Numbers
    - Punctuation
    - “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)

2. Contain at least eight characters.

3. The password should not be a word found in a dictionary (English or foreign)

4. The password should not be a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.

Try to create passwords that can be easily remembered. Develop a password using the first letters of a sentence or phrase that means something to you - like your national anthem or a slogan you have seen somewhere. ‘Helping People Celebrate Life’ would become ‘HlpPc&L1’.

(Note: this is an EXAMPLE. do not use this as your password!!!)

Password Protection Guidelines

1. Do not share passwords with anyone, including contractors or external service provider. All passwords are to be treated as sensitive, confidential information.

2. Password must be given to users in a secure manner, which limits the potential for unauthorised interception.

3. Passwords should never be written down or stored on-line without encryption.

4. Do not reveal a password in email, chat, or other electronic communication.

5. Do not speak about a password in front of others.

6. Do not hint at the format of a password (e.g., "my family name")

7. Do not reveal a password on questionnaires or security forms.

8. If someone demands a password, refer them to this document and direct them to the Information Technology Department.

9. Always decline the use of the "Remember Password" feature of applications (e.g. Outlook, Skype).

10. If an account or password compromise is suspected, report the incident to the Information Technology Department.

11. Initial passwords that have been assigned as original user-ID passwords must be changed at the first user log-on, whether the information system forces them or not.

12. Password protected screen-savers on all PCs and servers must be implemented. The screen-savers must automatically activate after at least ten (10) minutes. For systems that cannot have screen saver functionality, users must log off from their connection session when they plan to be away from their terminal for more than ten (10) minutes.

13. When not turned off, PCs and terminals must be protected from unauthorised use by appropriate controls, such as key-lock, BIOS password, etc.

14. Users must be forced to change passwords every thirty (30) days. System Administrator/IT Manager must enforce this through technical means by configuring password aging on systems. Where technically possible, user-ID access must be disabled upon thirty (30) days of inactivity (excluding super-user user-IDs).

15. If the password change cannot be enforceable by the system, manual changes at the user's place of work must be done once every 3 months.

16. All default passwords supplied by vendors must be changed following the installation of the software.

17. Passwords must be stored on secure systems with a one-way encrypted algorithm.

18. Users must log off from their connection session every time they complete their tasks.

19. Administrator password must be known to only authorized staff in the IT team. Administrator password must be changed regularly.

20. Passwords must not be visibly displayed on the screen when being entered.

21. Upon three (3) consecutive authentication failures, users must be locked out of the resource in which they are attempting to gain access, and must have to have their user-ID manually reset.

22. Connection sessions that are not active for more than thirty (30) minutes must automatically terminate both the application and network sessions. For those systems that cannot automatically terminate sessions, password protected screen savers or terminal locks must be implemented.

23. Terminals located in high-risk areas must automatically clear the terminal screen or shut down after not more than one (1) minute.

24. All computers, databases or applications that store user-ID and password information must be secured in the strictest manner. Access to the user-ID tables must be restricted to only authorised persons.

25. Passwords must be changed whenever there is an indication of possible System change or password compromise.

EMAIL SECURITY POLICY

Purpose:

The email security policy defines the best practices to be adopted with respect to email communication.

Scope:

This policy applies to all email users of the company.

Responsibility:

Only IT Department should alert the e-mail users of new virus attacks coming through email messages, and should provide preventive instructions. The e-mail users must act according to IT Service Department’s instructions in order to prevent their systems from being infected and damaged.

Policy:

1. Avoid sending credit card numbers, usernames and passwords by email unless these information are encrypted.
2. Do not disclose your email address to unknown web sites in order to reduce email spamming.
3. Do not open e-mail attachments which are received from unknown senders. These emails may contain viruses, e-mail bombs, or Trojan horse code. Such email should be deleted.
4. Delete spam, chain, and other junk email without forwarding.
5. It is a good practice to scan all email attachments received from people you know before downloading and opening them. Viruses and Spyware spread through email attachments by emailing themselves to email addresses listed in the address book and contact list.
6. Don’t access your email from an unsecured network or potentially compromised computers, like in an Internet Café or unauthorized computer/laptop.
7. Do not use foul, profane, obscene, offensive or defamatory language in your email
8. Do not send unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
9. Do not do any form of harassment via email such as intimidating, defaming, abusing and threatening as these may interfere with the legal rights of others.
10. Do not make unauthorized use, or forging, of email header information.
11. Do not send email messages to another individual or system who has explicitly asked user to stop sending email messages.
12. Do not create, distribute or forward "chain letters", or other "pyramid schemes” of any type.
13. Do not perform mass mailing of non-business-related messages.
14. Avoid sending large size attachments (greater than 20 MB) via email. Use alternatives like virus-free storage devices.
15. Do not use company email to engage in political, illegal, unethical and/or improper activities.

16. Unless appropriate permission is given by IT department or required strictly for business purposes, users must not access personal emails on the LUX* network.

Definition of terms

Email bomb

An email bomb is basically an attempt to overload an email server or, more specifically, a single inbox, with so many messages that it becomes unusable. Due to the way current messaging systems work, even shutting off the server or disconnecting it from the network would not help the situation, as the messages would simply wait for the system to come back on line.

Worm

A worm is a program that makes copies of itself; for example, from one disk drive to another, or by copying itself using email or another transport mechanism. The worm may do damage and compromise the security of the computer. It may arrive in the form of a joke program or software of some sort.

Trojan Horse

A Trojan horse, or Trojan, is a malicious application that appears as a legitimate file or helpful program but whose real purpose is, for example, to grant a hacker unauthorized access to a computer. Trojans do not attempt to inject themselves into other files like a computer virus. Trojan horses may steal information, or harm their host computer systems.

Spyware

Spyware is a type of malware (malicious software) installed on computers that collects information about users without their knowledge.

Email Spam

Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email. Clicking on links in spam email may send users to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments.

INTERNET ACCEPTABLE USE POLICY

Purpose:

This policy is intended to help employees of **LUX* Resorts & Hotels** to make the best use of the Internet resources at their disposal. They should understand the following:

1. The Organization provides Internet access to staff to assist them in carrying out their duties for the Company. It is envisaged that it will be used to lookup details about suppliers, products, to access government information and other statutory information. It should not be used for personal reasons.

2. Internet may only be accessed by using the Organization's firewall and router.

3. Internet access is provided and managed solely by the IT department.

When using the Organization's Internet access facilities employees should comply with the following guidelines.

DO

1. Do keep your use of the Internet to a minimum.
2. Do check that any information you access on the Internet is accurate, complete and current.
3. Do check the validity of the information found before using or distributing within the organization.
4. Do respect the legal protections to data and software provided by copyright and licenses.
5. Do inform the I.T. Department immediately of any unusual occurrence.

DO NOT

1. Do not download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
2. Do not download content from Internet sites unless it is work related.
3. Do not download software from the Internet and install it upon the Organisation's computer equipment.
4. Do not use the Organisation's computers to make unauthorised entry into any other computer or network.
5. Do not disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse Act 1990.
6. Do not represent yourself as another person.
7. Do not use Internet access to transmit confidential, political, obscene, threatening, or harassing materials.
8. Do not engage in unproductive or non-business activities such as online games, chat rooms, or other social activities.

Please note the following:

- All employees are subject to having their Internet activities monitored, recorded, and inspected.

- Any breach of the Organisation's Internet Acceptable Use Policy may lead to disciplinary action.

COMPUTER USAGE POLICY

Purpose:

This policy outlines the acceptable use of computer equipment.

Scope:

This policy applies to all users of computer equipment within **LUX* Resorts & Hotels**.

Policy:

1. Users must ensure their computers or laptops are locked or logged off before leaving their workstations unattended.
2. Unauthorised software should not be installed on computers and laptops.
3. Staff should not leave open files containing sensitive or critical information on their computers or laptops when leaving their workstations unattended.
4. Inappropriate sharing and releasing of information both internally and externally to the organisation may result in disciplinary or legal actions.
5. Use strong password and always change password when prompted by the system.
6. All employees, contractors and third party users should report any Information security events or suspected weaknesses in systems or services to the respective IT department as soon as possible.
7. Disciplinary or legal action will be taken against any employee using computers for unauthorised handling of information (e.g. copying, modifying, forwarding or destroying information).
8. Users should ensure neat and tidy cabling for their computers and should inform IT department if any cabling disorder is noticed at their workplace.
9. Users are responsible to maintain computers and laptops in good working condition and handle IT equipment with care so as to avoid theft and damage. In case of theft or damage to computers, laptops and/or other IT equipment, users must inform IT department immediately.
10. Employees should not establish connections to external networks (Internet service providers) using the organization’s systems without the prior approval of the Information Technology department.

WI-FI POLICY

Purpose:

This policy is intended to help employees of **LUX* Resorts & Hotels** to make the best use of the corporate WI-FI at their disposal. They should understand the following:

1. The Organization provides Wi-Fi access to staff to assist them in carrying out their duties for the Company.

2. This policy applies to all wireless devices in use by the organization or those who connect through a wireless device to any organizational network.

3. This policy is designed to protect the organizational resources against intrusion by those who would use wireless media to penetrate the network.

Configuration:
The SSID of the wireless device shall be configured in such manner so it does not contain or indicate any information about the organization, its departments, or its personnel including organization name, department name, employee name, employee phone number, email addresses, or product identifiers.

Usage:
When using the organization's Wi-Fi access point employees should comply with the following guidelines.

1. Ensure that request for corporate Wi-Fi access is made through respective head of department and approved by Group IT Manager.
2. All wireless access points and wireless devices connected to the organizational network must be registered and approved by Group IT Manager.
3. All wireless devices are subject to IT department audits and monitoring without notice.
4. All wireless devices must be checked for proper configuration by the IT department prior to being placed into service.
5. Only wireless devices approved by make and model shall be used.
6. Approved Wi-Fi users are provided with a unique login details. This must be kept confidential and not shared with anyone else.
7. Keep your use of the Wi-Fi to a strict minimum and always turn off Wi-Fi on devices when not in use.
8. Check that any information you access on the Internet is accurate, complete and current.
9. Check the validity of the information found before using or distributing within the organization.
10. Inform the IT Department immediately of any unusual occurrence.
11. Avoid connecting wireless devices containing company data to access points in public areas. (E.g. coffee shops, airport lounge, shopping malls, public transport etc.)

DO NOT

1. Do not download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
2. Do not download content from Internet sites unless it is work related.
3. Do not download unauthorised software/apps from the Internet and install it on the organisation's computer equipment or wireless devices.
4. Do not use the organisation's wireless network to make unauthorised entry into any other computer or network.

5. Do not disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse and Cybercrime Act.
6. Do not represent yourself as another person.
7. Do not use Wi-Fi access to transmit confidential, political, obscene, threatening, or harassing materials.
8. Do not engage in excessive, unproductive or non-business activities such as online games, chat rooms, or other social media activities.

Please note the following:

- All employees are subject to having their Internet activities monitored, recorded, and inspected.

- Team Members having access to free Wi-Fi facilities must also abide to the guidelines of the Wi-Fi Policy and Internet Acceptable Use Policy.

- Any breach of the Organisation’s Wi-Fi Policy and Internet Acceptable Use Policy may lead to disciplinary action.