PHOENIX TOWER
INTERNATIONAL

PHOENIX TOWER INTERNATIONAL'S INFORMATION SECURITY POLICY

EFFECTIVE AS OF AUGUST 15TH 2023

PURPOSE

Phoenix Tower US Holdings, L.P. and its subsidiaries and affiliates worldwide (collectively "PTI," "Phoenix Tower" or "Company"), are committed to protecting information security and continued learning and improvement, as set forth in this Information Security Policy (the "Policy"). The scope of this Policy is intended to be comprehensive and will include Company requirements for the security and protection of PTI assets, including Personally Identifiable Information ("PII"), throughout the Company and its approved vendors both on and off work premises. All Employees must review and follow the information contained in this Policy.

SCOPE

This Policy applies to all Phoenix Tower Employees and vendors who support or interact with Phoenix Tower and its information assets. Each section of this Policy applies to specific aspects of PTI's information security program.

DEFINITIONS

- **Confidential Information: includes but is not limited to** all material, non-public, business-related information, intellectual property rights, trade secrets, business know-how, whether in written or oral form, whether or not it is marked as such, relating to such matters as business strategy, processes, financials, marketing plans, contracts, and/or technology. Examples include but are not limited to:
    - Contracts, both executed and in draft form;
    - Marketing materials under development; or
    - Sales or revenue projections.
- **Information Security:** the processes and methodologies that are designed and implemented to protect, print, electronic or any other form of confidential, private, or sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.
- **Employee:** an identified or identifiable natural person who is acting as a PTI director, officer, team member, Employee, contractor, or consultant, whether full time or part-time, on a temporary or permanent basis.
- **End User Facing Devices:** any technology tool or device used by a PTI Employee to store information or access PTI systems, including email. Examples of End User Facing Devices include computers, laptops, smart phones, external hard drives, and USB storage.
- **Personally Identifiable Information ("PII"):** any data that could potentially identify a specific individual, such as name, address, email, financial information, social security number, passport number, etc.

POLICY OVERSIGHT

Phoenix Tower regards Information Security as one of the most important aspects of its business.

- Phoenix Tower senior management will lead by example by ensuring information security is given a high priority in all current and future business activities and initiatives.
- This Policy and each of its appendices will be reviewed annually by the Global General Counsel to ensure that they are relevant and up-to- date and revised, as necessary, to ensure they are adequate in light of evolving legal obligations, technology and business needs.
- Management will communicate policy revisions to all staff by various means, such as electronic updates, briefings, training, newsletters, etc.

To meet or exceed these objectives, the following practices have been put into place:

- Employees sign a notice of receipt, review, and acknowledgement of the Information Security Policy when hired/retained.
- Staff awareness will be periodically reinforced to make information security issues a priority.
- Information Security training is mandatory from the beginning, starting with employee onboarding. Any technical training should be relevant to the responsibilities of the job function. When staff members change jobs or functions, their Information Security needs must be reassessed, and new training should be provided as a priority.

1. SECURITY ORGANISATION

1.1 DEFINITION OF ROLES AND RESPONSIBILITIES

The following roles are established in PTI related to Information Security:

ROLES	RESPONSIBILITIES
Director of Information Technology	Determine the security requirements of the services provided by assessing the impact of an incident affecting the security of the services to the detriment of availability, authenticity, integrity, confidentiality or traceability.
Director of Information Technology	Determines the security requirements of the information processed, assessing the impact that an incident affecting the security of the information would have on the availability,

	authenticity, integrity, confidentiality or traceability.
Director of Information Technology	Shall determine the decisions to satisfy the information and service security requirements, supervising the implementation of the necessary measures and reporting on these issues.
Sr Information Technology Manager	Responsible for developing the specific way of implementing security in the systems and for the supervision of the daily operation of the systems, and may delegate to administrators or operators under his responsibility.
Sr Information Technology Manager	Responsible for the technical security tasks, who executes them.

2. PERSONALLY-IDENTIFIABLE INFORMATION

This section is intended to guide the protection of PII collected from Landlords, Tenants, sales leads, and Employees, and it will help Employees determine what information can be disclosed to non-Employees, as well as the relative sensitivity of information that will not be disclosed outside of Phoenix Tower without appropriate authorization.

2.1 Definitions

Phoenix Tower recognizes its need to maintain the confidentiality of PII and understands that such information is unique to each individual and is generally limited to data that is relevant and necessary for its purposes. The PII covered by this Policy may come from various types of individuals performing tasks on behalf of the Company and includes Employees, applicants/candidates, independent contractors, and any PII maintained on its customer base. PII includes all identifiable information about Landlords, Tenants, sales leads, and Employees:

- Personal contact information (phone numbers, addresses, etc.);
- Social Security Numbers (or their equivalent issued by governmental entities outside the United States);
- Taxpayer Identification Numbers (or their equivalent issued by governmental revenue entities outside the United States);
- Employer Identification Numbers (or their equivalent issued by government entities outside the United States);
- State or foreign driver's license numbers or copies of identification cards;

- Passport numbers or copies of passports;
- Dates of birth;
- Corporate or individually held credit or debit transaction card numbers (including PIN or access numbers) maintained in organizational or approved vendor records; or
- PTI or business partners' banking account information.

PII may reside in hard copy or electronic records; both forms of PII fall within the scope of this Policy.

2.2 Storing and Handling Information that Contains PII

Electronic PII

PII can be saved electronically by a variety of methods and on a variety of End User Facing devices, included but not limited to the following:

- Mobile computing devices (i.e. laptops, smartphones, tablets, computers, PDAs,etc.).
- E-mail, internet and instant message programs that store, process or transmit data.
- Removable electronic media, such as USB drives, CD drives, external hard-drives, etc., should only be used for non-sensitive PII. Sensitive PII, such as Social Security Numbers, Passport information, and banking or other financial data should not be saved on removable electronic media.
- Local and Cloud PTI-owned servers.
- Third party cloud-based servers.

This Policy section sets forth the requirements and approval process for End User Facing Devices that are owned, managed, or leased by PTI. Any End User Facing Devices that are not owned, leased, or managed by PTI shall not be allowed to access or remove any local servers containing PII, unless authorized, in writing, by the Global General Counsel.

- **Mobile computing devices (i.e. laptops, smartphones, tablet computers, PDAs, etc.)** – PII can be saved on mobile computing devices, but such devices should be password protected, encrypted, and have remote wipe capabilities. This is not a preferred method of storing PII and information stored on mobile computing devices should be viewed as a temporary storage location and the PII should be moved to a PTI server as soon as possible.
- **Email, internet, and instant messaging programs –** The Company does not recommend transmitting PII via the internet or instant messaging programs. When PII is to be transferred via email, the following steps must be taken to ensure a secure transmission and minimize the risk of a breach after such PII is confirmed to have been saved to the local server:
    1. Password protect the document, whether pdf, word or excel. If the document is in a format that is not easily protected (i.e., gif or jpeg), convert the document into a pdf file, password protect in this format and

resave it. The "original" format can be deleted at this time and removed from the trash.

2. Email the document with the language "**CONFIDENTIAL**" as a label following the subject
   name in the subject line.
3. Contact the recipient by phone to confirm the recipient has received the email and provide them with the password. ***NEVER SEND THE PASSWORD IN EMAIL ***
4. Delete the attachment from the sent email.

Sensitive PII, such as Social Security Numbers, Passport information, and banking or other financial data should **not** be transmitted in email.

If any PII is received by PTI via internet or instant messaging programs, or any other insecure means, the information should be transferred immediately to the PTI server (first preference) or moved to the storage of a mobile computing device and then permanently deleted from the program in which it was received.

- **Removable electronic media –** PII can be saved on removable electronic media, such as USB drives, for the purposes of transporting information between media. The removable media devices should be password protected and encrypted. This is not a preferred method of storing PII. Information stored on removable electronic media should be viewed as a temporary storage location and the PII should be moved to a PTI server as soon as possible and removed from the removeable media. Sensitive PII, such as Social Security Numbers, Passport information, and banking or other financial data should **not** be saved in removable electronic media.
- **Local or Cloud PTI-owned server** – The preferred place for storage of all PII is on PTI-owned local or cloud- based servers and this method of storage should always be used first when available. All folders and data containing PII must be clearly labelled as such and access to these folders will be restricted only to those Employees that are required to have access in the day-to-day function of their jobs.
- **Hardcopy storage (on-site)** – PII stored in the office locations should be secured in locked drawers and preferably behind locked doors if possible. Access to these locations should be restricted to those Employees requiring the information in the performance of their daily work-functions. Keys to such secured locations should be kept only by the department head and any access provided to Employees documented in a log format. In no ordinary event are any documents containing PII to be taken out of the office and any such instances requiring the removal of PII from the office will require the approval of the CEO. All information, data and documents containing PII are to be clearly labeled so that all users are aware of the ownership, classification and value of the information. Information, data and documents containing PII will be transported

safely and destroyed securely, to protect from unintentional disclosure. Information, data and documents containing PII will be stored securely when not in use.

- **Hardcopy storage (off-site) –** Storage of PII in hardcopy format off-site is not generally permissible without the written approval of the CEO. Data containing PII in hardcopy format should not be sent to off-site storage facilities as part of the site files, and under no circumstances are such data to be stored in Employees' homes. All information, data and documents containing PII are to be clearly labeled so that all users are aware of the ownership, classification and value of the information. Information, data and documents containing PII will be transported safely and destroyed securely to protect from unintentional disclosure. Information, data and documents containing PII will be stored securely when not in use.
- **Hardcopy Transportation –** When PII needs to be transported out of the office premises under approved situations, it should only be done by direct Employees of PTI. Sufficient care should be taken to ensure that the data containing PII is secured (locked briefcase, etc.) and that such data is always in the possession of the Employee while in transport.
- **Hardcopy Print Outs –** The printing of data containing PII and stored electronically should be avoided as much as possible. In situations where this is not possible, the Employee printing the data will need to receive prior approval from the department head, stating what materials are being printed and for what reason. The Employee will also be responsible for the destruction of the hard copy printouts, and will provide the department head with a statement containing the date of destruction, description of material destroyed, and the method used.

2.3 Access to PII by Employees

Each department head is responsible for identifying and maintaining a list of users in their department that should have access to files (electronic or hard copy). The list should be updated as required and at a minimum should be reviewed yearly and upon a personnel event (e.g., hiring, separation, termination, promotion). The list will be provided to the IT department who in turn will be responsible for ensuring that access to softcopy files containing PII are restricted in accordance with the list. Each department head will be responsible for ensuring that access to the hardcopy files containing PII are restricted in accordance with the list. Department heads and/or the managers they designate must review user access upon any change in an affected individual's job roles and responsibilities, or Employee/independent contractor status (including but not limited to termination) and communicate any changes timely to IT.

2.4 Regulatory Requirements

It is the policy of the Company to comply with any international, federal or State statutes and regulations regarding the access, use, storage, and retention of PII. Phoenix Tower Legal and/or Compliance department(s) shall oversee all regulatory compliance issues. If any provision of this Policy conflicts with a statutory requirement of international, federal or state law governing PII, the Policy provision(s) that conflict shall be superseded.

2.5 Training

All new hires entering the Company are provided with introductory training regarding the proper management and protection of PII and are provided a copy of this Policy and implementing procedures for the department to which they are assigned (if any). Employees in positions with regular ongoing access to PII or those transferred into such positions are provided with training reinforcing this Policy and procedures for the maintenance of PII data and shall receive training regarding the security and protection of PII data and company proprietary data at least annually. The training will be led by the IT department and will be part of the new Employee orientation in the case of new Employees. If an existing Employee is added to the PII access list, the Employee will receive a separate training as to the provisions of this Policy.

2.6 Confirmation of Confidentiality

All Company Employees must maintain the confidentiality of PII as well as company Confidential Information to which they may have access and understand that such PII is to be restricted to only those with a business need to know.

2.7 PII Data Breaches/Security Incidents

If an Employee becomes aware of any use, access, or transfer of PII that conflicts with this Policy or any security incident, the Employee should report it to the Phoenix Tower Legal Department immediately. Databases or data sets that include PII may be breached inadvertently or through wrongful intrusion. Please see Section 6 of this Policy for further information.

2.8 Violations of PII Policies and Procedures

Phoenix Tower views the protection of PII data to be of the utmost importance. Infractions of this Policy or its procedures will result in disciplinary actions, which may include suspension or termination in the case of severe or repeat violations.

2.9 Monitoring Use of Computer Systems

The Company has the right and capability to monitor electronic information created and/or communicated by persons using Company computer systems and networks, including e-mail messages and usage of the Internet. It is not the Company policy or intent to continuously monitor all computer usage by employees or other users of the Company computer systems and network. However, users of the systems should be aware that the Company may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g., site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with Company policy. Use of the Company's computer systems and networks will be deemed an as affirmative acknowledgement and consent of the above described monitoring.

3. ACCEPTABLE USE

The purpose of this section is to ensure the acceptable use of computer equipment owned, leased, or managed by Phoenix Tower. Inappropriate use exposes Phoenix Tower to risks including virus attacks, compromise of network systems and services, reputational harm, and legal issues.

3.1 General Use and Ownership

- Users will be aware that the data they create or applications using the data on the corporate systems remains the property of Phoenix Tower. Employees should have no expectation of privacy for their activities while using PTI computer equipment and no expectation of ownership including upon separation from the Company.
- For security and network maintenance purposes, authorized individuals within Phoenix Tower may monitor equipment, systems, and network traffic at any time.
- Phoenix Tower reserves the right to audit networks and systems on a periodic basis to ensure compliance with this Policy.

3.2 Security and Proprietary Information

- Information kept on Phoenix Tower systems that contain PII will be clearly labeled as such in accordance with the Personally Identifiable Information section of this Policy. Users will strive to keep this information secure.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security and integrity of their passwords and accounts.
- Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses or malware.
- Systems storing Phoenix Tower confidential information, or that are used for information processing, are not to be removed from the Phoenix Tower

premises without official management approval.
- Employees should not use web browser auto-populate features or other features which save user ID and password information to online based business applications.

3.3 Prohibited Activities

- Engaging in any activity that is illegal under local, state, federal or international law while utilizing Phoenix Tower-owned resources.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management will be consulted prior to the export of any material that is in question.
- Using a Phoenix Tower computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Circumventing user authentication or security of any host, network or account. Unauthorized use of a network ID other than your own is strictly prohibited.
- Unauthorized attempts to circumvent network security, data protection, password security or installing/using software designed to circumvent any security or policy created and implemented by Phoenix Tower.
- Attempting to tamper with or manipulate another Employee's network communication or files.
- Violating any copyright laws and their fair use provisions. This includes copying or "pirating" software or
  violating software licenses/agreements.
- Installation of unofficial applications on any Phoenix Tower assets without prior consent of IT.
- Disclosing confidential information and/or trade secrets.
- Users shall not purposely engage in gaining access to Company systems for which they do not have authorization, or a business need to know.

4. **EMAIL USE**

This section is intended to provide guidelines for acceptable use of email and outline email retention procedures.

4.1 Permitted Use

- Company email and email systems should be used for business purposes only and must be consistent with PTI's policies and procedures for ethical conduct, safety, and compliance with applicable laws and business practices. Any personal communications on company email must be limited.
- Employees shall have no expectation of privacy in anything they store, send or receive on the Company's email system. PTI may monitor messages without

prior notice.
- Employees must be complaint with Multi-Factor Authentication.

4.2 Email containing PII

- If PII is to be transferred via email the following steps must be taken to ensure a secure transmission and minimize the risk of a breach after such PII is confirmed to have been saved in the local server:
    1. Password protect the document, whether pdf, word or excel. If the document is in a format that is not easily protected (i.e., gif or jpeg), convert the document into a pdf file, password protect in this format and resave it. The "original" format can be deleted at this time and removed from the trash.
    2. Email the document with the language "**CONFIDENTIAL**" as a label following the subject
    name in the subject line.
    3. Contact the recipient by phone to confirm the recipient has received the email and provide them with the password. ***NEVER SEND THE PASSWORD IN THE SAME EMAIL AS THE PII***
    4. Delete the attachment from the sent email.

- Sensitive PII, such as Social Security Numbers, Passport information, and banking or other financial data should **not** be sent in an email.
- If any PII is received by PTI via email, internet or instant messaging programs, the information should be transferred immediately to the local server (first preference) or moved to the storage of a mobile computing device and then permanently deleted from the program in which it was received.

4.3 Prohibited Email and Communications Activities

- Using PTI email for non-PTI related commercial uses or frequent personal use.
- Automatically forwarding PTI email to third-party email systems or platforms.
- Deleting or altering the system generated legal disclaimer message attached to every PTI email.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising or solicitation material to individuals who did not specifically request such material (email spam).
- The creation or distribution of any disruptive or offensive messages. Employees who receive any emails with this content from any Phoenix Tower Employee will report the matter to their supervisor immediately.
- Using non-Phoenix Tower email accounts (Hotmail, Gmail, et. al.) for official Phoenix Tower business, or forwarding emails received in Phoenix Tower email accounts to personal or non-Phoenix Tower email accounts (Hotmail, Gmail, et. al.).

- Subscription to electronic services or other contracts using PTI email addresses without a valid business reason.

4.4 Mobile devices

- Employees must obtain prior approval from their manager or supervisor before attempting to access PTI email via personal mobile devices.
- Phoenix Tower provides access to email via mobile personal devices consistent with this Policy. Phoenix Tower is not liable for lost data in the event a device is erased (either due to user error or by security features that are implemented). This policy applies to all handheld End User Device and any other device that may access Phoenix Tower email services and/or protected Phoenix Tower data. Compliance with this Policy is a requirement for all handheld computing devices storing or accessing Phoenix Tower protected data.
- Users that use a handheld computing device to access Phoenix Tower email, data, records or documents should implement the following security features to the extent they are available on the device:
    - Be configured to log-off or power down no longer than ten (10) minutes after the last user activity.
    - Require a power-on password or passcode.
    - Require a minimum password length of four (4) characters or keys.
    - Provide a device reset (data erasure) if an incorrect password is entered more than eight (8) consecutive times, when technically feasible.
    - Device must be encrypted.

- Users that use a handheld computing device to access Phoenix Tower email, data, records or documents should bring their device to IT to ensure these security features are implemented.

4.5 Equipment Disposal

Prior to disposal or transfer, all handheld computing devices and associated memory cards should be completely cleared of all Phoenix Tower data. Upon termination of an Employee's access to Phoenix Tower systems, the individual will bring his/her handheld computing device to IT so that IT can remove any Phoenix Tower data from the device.

4.6 Reporting

- Loss, theft, or any unauthorized use of a handheld End User Device that has been used to store or access protected Phoenix Tower information constitutes a disclosure and must be reported to Phoenix Tower IT.

- IT will coordinate with Legal and the user's supervisor to determine the extent to which a PTI-owned or personal End User Device should be wiped or cleared upon loss or theft and at the end of the user's employment with PTI. If it is determined that a remote wipe is necessary and possible, IT will attempt to limit the data erased to only Phoenix Tower information to the extent technically possible on the PTI-owned devices and/or devices wherein refunds apply.

5. USE OF THE INTERNET

The Company will provide Internet access to employees and contractors who are connected to the internal network and who have a business need for this access.

The Internet is a business tool for the Company. It is to be used for business-related purposes such as: communicating via electronic mail with suppliers and business partners, obtaining useful business information, and research relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving, or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature for "chain letters" or any other purpose which is illegal or for personal gain.

6. PERSONNEL

The purpose of this section is to reduce the risk of human error, theft, fraud, or misuse of facilities. Because the security of our information assets is a critical component of our business model, it is vital that all Phoenix Tower Employees be subjected to certain standards to ensure credibility and security.

6.1 Storing PII on Company Systems

- Notwithstanding Phoenix Tower's respect for Employee's privacy in the workplace, it reserves the right to have access to all information created and stored on Phoenix Tower's systems.
- Phoenix Tower has the right to monitor all information received, stored, transmitted, and/or created on
  Phoenix Tower's systems.

6.2 Sharing Confidential Information

- Confidential Information will be shared only with other authorized persons.
- Organization information has its own individual levels of sensitivity and must not be divulged to staff that do not have authorization to access that information.
- All data and information not in the public domain, relating to Phoenix Tower's business and its Employees, must remain confidential at all times.
- Confidential information must not be divulged to family members who do not

have clearance to receive such information.

7. PHYSICAL SECURITY

This section prohibits unauthorized physical access to Phoenix Tower premises and information and prevents damage to or interference with normal business operations. This Policy also covers all physical security of entrances, office working facilities, and other critical areas that must be secure in order to protect assets.

7.1 Physical Security

- Security doors, badge readers, and PIN keypads are in use to secure areas with critical information. Only authorized Employees may enter these secure areas.
- Staff will be electronically monitored according to which areas that they have been granted access to. This is to mitigate the dangers of theft, vandalism, and unauthorized use of the systems.
- Areas where secure information is handled (including information processing and computing facilities) will be subjected to strict access controls to ensure that no unauthorized Employees or people outside of the organization are granted access.

7.2 Securing Unattended Workstations and Working Facilities

- Equipment is always to be safeguarded appropriately, especially when left unattended.
- Prior to leaving your desk, if your desk will be out of sight, your computer must be logged off or locked in order to prevent unauthorized access.
- Printers and fax machines will be cleared of sensitive data daily. Sensitive documents sent to printers or fax machines should be secured as soon as they are printed.

7.3 Lending Keys, Security Codes, or Security Access Badges to Others

- The use of keys, whether physical or electronic, to access secure areas is to be strictly limited to the Employee to which the keys were assigned. The lending of keys, security codes, or security access badges to non-PTI Employees and/or outside persons is prohibited.
- Failure to abide by this Policy could be viewed as a security breach and is subject to disciplinary action.

7.4 Handling Strangers on the Premises

- If a stranger is not accompanied by an Employee of Phoenix Tower, Employees

will challenge the stranger's presence on the organization's premises.

8. ACCESS CONTROL

A fundamental component of our Information Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

8.1 User System and Network Access – Normal User Identification

All users will be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with management & supervisory personnel and/or any other employee whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Password must be complex. :
  - The minimum length of a password must be 8 characters.
  - It must consist of a combination of alphanumeric characters (upper and lower case letters, numeric digits and special signs).
  - Lower case alphabet.
  - Upper case alphabet.
  - Symbols: . : { } ! @ # $ % ^ & * ? _ ~ -
  - Numbers from 0 to 9.
  - It should not contain consecutive identical characters.
  - As a recommendation, the password should not be the same as any of the last 5 passwords used.
- That is, do not use any common name, noun, verb, adverb, or adjective. These easy passwords can be easily cracked using standard "hacker tools".
- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the terminal.
- Password must be changed every 60 days.
- User accounts will be frozen after 5 failed logon attempts.
- Logon IDs and passwords will be suspended after 20 days without use.

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting, or modifying a password file on any computer system is strictly prohibited.

Users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this document.

Employee Logon IDs and passwords will be deactivated as soon as possible if the employee is separated, terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the Company office.

Supervisors / Managers shall immediately and directly contact the Company IT department to report any change in employee status that requires terminating or modifying employee logon access privileges.

Employees who forget their password must call the IT department or follow the tools provided for IT to get a new password assigned to their account. The employee must identify himself/herself by (e.g., employee number) to the IT department.

Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

8.2 System Administrator Access

System Administrators, network administrators, and security administrators will have high privilege access to host systems, routers, hubs, and firewalls as required to fulfill the duties of their job.

All system administrator passwords will be **DELETED** immediately after any employee who has access to such passwords is separated, terminated, fired, or otherwise leaves the employment of the company. Employees placed on administrative or disciplinary leave shall have their passwords suspended until active employment status is restored.

8.3 Special Access

Special access accounts are provided to individuals requiring temporary system administrator privileges to perform their job. These accounts are monitored by the Company and require the permission of the user's Company IT. Monitoring of the special access accounts is done by entering the users into a specific area and periodically generating reports to management. The reports will show who currently has a special access account, for what reason, and when it will expire. Special accounts will expire in 2 days and will not be automatically renewed without written permission.

8.4 Connecting to Third-Party Networks

This policy is established to ensure a secure method of connectivity provided between the Company and all third- part companies and other entities required to electronically exchange information with the Company.

"Third-party" refers to vendors, consultants and business partners doing business with the Company, and other partners that have a need to exchange information with the Company. Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of the Company. The third-party Company will ensure that only authorized users will be allowed to access information on the Company network. The third-party will not allow Internet traffic or other private network traffic to flow into the Company network. A third- party network connection is defined as one of the following connectivity options:

- A network connection will terminate on a Firewall and the third-party will be subject to standard company authentication rules.

This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re- designed as needed.

All requests for third-party connections must be made by submitting a written request and be approved by the IT department.

8.5 Connecting Devices to the Network

Only authorized devices may be connected to the Company network(s). Authorized devices include PCs and workstations owned by the Company that comply with the configuration guidelines of the Company. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach to the network: non-company computers that are not authorized, owned and/or controlled by Company. Users are specifically prohibited from attaching any non-company device like laptops, computers, external hard drives, phones, tablets to the Company network.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices (e.g., thumb drives and writable CDs).

8.6 Remote Access

Only authorized persons may remotely access the Company network. Remote access is provided to those employees, contractors and business partners of the Company that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connections can be remote PC to the network or a

remote network to company network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.

8.7 Unauthorized Remote Access

The attachment of hubs to a user's PC or workstation that is connected to the Company Local Area Network (LAN) is prohibited without the written permission of the Company. Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

9. INCIDENT RESPONSE AND DATA BREACH REPORTING

In the event of a security incident, it is important that Phoenix Tower Employees are able to identify and respond appropriately. Each potential incident will be investigated to a level deemed appropriate by Legal and IT. Properly and timely responding to information security incidents will help to protect Phoenix Tower's assets.

9.1 Reporting

- Each Employee is responsible for reporting all identified or suspected Information Security weaknesses, including but not limited to potential or actual PII data breaches, immediately to IT and/or Legal/Compliance:
    - Hotline: 1-844-348-5247 or https://secure.ethicspoint.com
    - Email: privacy@phoenixintnl.com
- A breach of confidentiality, or unauthorized disclosure of Phoenix Tower Confidential Information, is also considered an Information Security incident and must be reported as outlined above.
- IT will record reported security incidents to monitor both the types of security incidents as well as the volume of incidents occurring at Phoenix Tower.
- Evidence relating to an information security breach must be properly collected as directed by the IT department manager and forwarded to the IT department. It must be collected to comply with statutory, regulatory or contractual obligations and avoid violations? of criminal or civil law.
- After conducting an initial investigation, the IT department manager will determine whether or not the event is indeed an information security incident. If a security incident has occurred, Legal will determine if the incident constitutes a data breach for which reporting is required, and of data breaches involving PII.
- Legal will maintain a record of reported security incidents that constitute a data breach.
- Information relating to information security incidents may only be released by authorized persons. Employees may not release any information regarding a security incident outside of PTI without the express permission of the Legal team.

- Following the incident or data breach, the IT department will be responsible for conducting a meeting with all affected/applicable Employees and parties to review the results of the investigation and to discuss the root cause of the Incident. Any Employees involved in the discovery or investigation of a
- security incident are required to attend this meeting.
- Phoenix Tower Employees or third-party contractors involved in a security incident or found to have violated Phoenix Tower Information Security Policy, regardless of intent, will face a disciplinary panel, who will determine fault, corrective and other appropriate action.

9.2 Notification of the data breach

- **Notification to the supervisory authority:** PTI, as Data Controller, shall notify the National Supervisory Authority immediately (as soon as it becomes aware of the incident) and, at the latest, within 72 hours of becoming aware of the incident including the hours elapsed during weekends and public holidays. For communication, PTI should use the form of notification, by country, provided in **Incident Management Procedure**.

- **Notification of data subjects:** PTI, as Data Controller, must notify those affected of security breaches when the breach could have a negative impact on their personal data or privacy.

10. PRIVACY BY DESIGN

PTI undertakes to adopt the technical and organisational measures necessary to give concrete effect to the provisions and principles of data protection and thus to guarantee the rights of data subjects. In order to do so, the PTI must consider the adoption of the necessary legal, technical and organisational measures from the development and design phase of the products and services or from the initial moment when any project, initiative or idea involving the Processing of personal Data is proposed by the PTI.

For the implementation of legal measures, the Responsible of the data protection issues must be consulted, and for technical and organisational measures, the head of the IT department must be consulted.

To this end, each area, project or new process manager must ensure that privacy is implemented by design and by default, in addition to complying with the basic principles of the regulation.

11. ADDITIONAL SECURITY MEASURES

To protect the integrity, confidentiality and availability of information, PTI has implemented the following security measures:

11.1 Vulnerability and malware detection and management.

In relation to the continuous process of vulnerability detection and management, this security measure is implemented to identify, assess, address and report security vulnerabilities in systems. To this end, PTI has implemented Microsoft Defender and Zscaler tools for the detection and management of vulnerabilities and malware.

11.2 Patch Management Policy

In relation to patch management, PTI has developed a patch management policy, which states that patches published by Microsoft will be installed as Intune, Zero day. Network Access Control.

11.3 Encryption Mechanisms

In relation to encryption mechanisms, PTI has implemented such mechanisms, both in the database and on the hard disk of laptops. In this way, the information stored on the devices is not accessible in the event unauthorized access. Encryption mechanisms are used, both in the databases and in the hard disk of laptops. In this case, an erasure mechanism has been implemented, in the event of loss or theft of equipment that in addition to data encryption security measures, remote erasure can be performed.

11.4 Account Management.

In relation to account management. PTI has implemented mechanisms referred to as Privileged Identity Management (PIM) and Privileged Access Management (PAM).