AIP REALTY TRUST

CYBER SECURITY POLICY

1. PURPOSE

AIP Realty Trust (the "**Trust**") is committed to achieving a targeted level of protection from internal and external cyber security threats, and accordingly, will implement ongoing governance, policies and practices which address the following objectives:

- Ensure business continuity, including the recovery of data and operational capabilities in the event of a security breach.
- Ensure compliance with all applicable laws and regulations.
- Ensure compliance with internal policies, controls, standards and guidelines.
- Ensure the confidentiality, privacy and integrity of the Trust's information.
- Establish controls for protecting the Trust's information and information systems against theft, abuse and other forms of harm or loss.
- Motivate administrators and employees to maintain responsibility for, ownership of, and knowledge about information security.
- Ensure the protection of the Trust's data and information assets.
- Ensure the availability and reliability of the network infrastructure, systems and the services.
- Ensure that external service providers are made aware of, and comply with, the Trust's information security needs and requirements and continuously assess whether they maintain an acceptable cyber security posture.
- Balance the need for the above with the investment and policy constraints required to achieve an appropriate level of protection while maintaining business agility.

2. SCOPE

This policy applies to all permanent and temporary employees of the Trust, as well as the Board of Trustees. It also applies to independent contractors, consultants, vendors, suppliers, agents and other users of the Trust's IT resources (together referred to as "**users**"), wherever they may be located. The policy is structured in the following categories:

A. Leadership and Governance;
B. Human Factors;
C. Information Risk Management;
D. Business Continuity;
E. Operations Technology; and
F. Legal and Compliance.

Any breach of this policy is a serious offence and will result in the consideration of appropriate sanctions up to and including termination of employment, contract or legal action.

3. DETAILS

A. Leadership and Governance

Cyber security is a strategic business matter for the Trust. Accordingly:

- The development and promulgation of a cyber security plan for the Trust is the responsibility of Chief Financial Officer.
- The implementation of the cyber security plan is the responsibility of Chief Financial Officer, who is accountable for the results.
- Oversight of the effectiveness of the cyber security plan is the responsibility of Chief Financial Officer.
- Cyber risk should be reflected in reports and updates to the Board of Trustees at least quarterly.
- Cyber risk should be considered by all levels of leadership where changes to business processes, including but not limited to, the information and technology environment.

B. Human Factors

Authorized Use: The Trust prohibits use of IT resources for any purpose other than business, unless otherwise stated in this policy. All users must behave honestly with vigilance, respect the intended business use of technologies and comply with software licenses, property rights, user agreements, confidentiality and legal rights. Users must comply with the Trust's internal policies and all applicable law when using its IT resources, including without limitation, privacy and intellectual property laws.

Limited personal use is acceptable, provided that it does not affect job performance, is not for personal financial, commercial, or third party gain and if the user adheres strictly to this policy. The Trust's systems must not be used for the creation or distribution of any material considered inappropriate, offensive, threatening, abusive, defamatory, unlawful, sexually explicit, sexist, racist, discriminatory, embarrassing, fraudulent or disrespectful to others, or that could potentially breach the corresponding software license agreement. The Trust restricts all users from using the Internet to perform any task contrary to the law or knowingly accessing websites with content that is illegal, obscene, hateful, defamatory, indecent, objectionable or inappropriate.

To maintain the integrity of the Trust's public image and reputation and to prevent the unauthorized or inadvertent disclosure of sensitive, confidential or personal information, employees must exercise caution and care when using any system, service or technology platform, both internal and external, including e-mail or third party services, such as Cloud-based and social media. Personally identifiable information, which is any data that could identify a specific individual, should not be transmitted via e-mail or shared using any other service (with the exception of site level or corporate human resources ("**HR**") or legal groups) without approval by the appropriate site or corporate HR group. Employees must also exercise caution against suspicious messages and technologies, which are often intended to bait a user into a malicious cyber event.

Passwords: Users are responsible for utilizing effective passwords and for keeping those passwords secret and secure. Employees must not appropriate, use or disclose someone else's login or password without prior authorization by the employee's supervisor or HR. In addition, employees should ensure that the function of retaining passwords by Trust-issued computers is disabled. The IT department or designated responsible individual(s) (in both instances the "**IT department**") will support the mechanisms that evaluate the strength of passwords and define the password change frequency for every type of applications, services and devices supported by the Trust, along with other mechanisms to strengthen the way users identify themselves when accessing the Trust's IT resources, such as multifactor authentication.

Confidentiality: The Trust prohibits the release of confidential information to any third party, or use of confidential information, except as required in the performance of Trust-related work approved by the employee's supervisor and in accordance with the terms of any applicable confidentiality agreement.

Privacy: Users should have no expectation of personal privacy in anything they create, store, send or receive by e-mail or when using any corporate application if they use equipment (e.g. mobile device, computers) owned or provided by the Trust. The nature of the Trust's business requires effective monitoring of activities on its network, including the conduct of users. The Trust reserves the right to review and collect all information contained in e-mails, whether or not stored solely in personal folders on the computer operated by the user, and in all equipment owned or provided by the Trust.

Ownership: Data and employees' work and work products belong to the Trust, including all messages sent or received, regardless of the device or application used to produce, send or receive it.

Security: Used unwisely, the Internet can be a source of security problems that can cause significant damage to the Trust. Users must:

- Apply best practices to prevent any form of computer virus.
- Only access websites, applications or systems for which they have authorization.
- Only use approved services for the uploading or sharing of Trust data.

Awareness, Communication and Training:

- To mitigate the risk of unintentional disclosure of confidential information by employees, HR will refer newly onboarded employees to this policy and will require formal acknowledgement that it has been read, is understood and will be applied.

- To mitigate the risk of unintentional disclosure of confidential information by employees, cyber security training and awareness sessions will be provided as an integral part of employee onboarding and ongoing employee development. In addition, acknowledgement of this policy, that it is understood and that the employee agrees to apply it will be included in the annual sign off along with the code of conduct.
- Upon a change in status, including promotion, transfer or termination of employment, the employee's network and physical access privileges will be modified as appropriate in a timely manner.
- Third parties, vendors, suppliers, partners, contractors, service providers or customers with connectivity to the Trust's internal network or access to the Trust's data must comply with this policy.

C. Information Risk Management

The Trust will develop, maintain and periodically update risk appetite statements that:

- Articulate its position with respect to cyber risk.
- Specifically address the degree of protection that the Trust is targeting and how it will be measured.

The Trust will develop, maintain and periodically update an inventory of major types of information and systems on the basis of criticality to the business. This list, on a priority basis, will be used to formally assess the degree of cyber protection that the Trust has, the target degree of protection, as well as the plans that are in place to achieve the desired level as appropriate. The target level will reflect the nature of the information or application as well as the risk appetite defined above.

D. Business Continuity

The IT department is responsible for the development and promulgation of standards and guidelines for acceptable IT-related business continuity and disaster recovery plans.

Business continuity and disaster recovery plans should be developed and aligned at two levels:

- The application owner - normally the individual who is regularly the business process lead and is the person having authorized the deployment of the application, is responsible for developing a continuity plan for business applications.
- IT is responsible for developing a continuity plan for the overall IT environment, including data backup and recovery.

E. Operations Technology

Data, Applications, Networks, New Software and IT Equipment: To prevent the deployment of software and IT equipment that could compromise the security of the Trust's IT infrastructure, the IT department will establish standards for the development, acquisition, installation and approval of all new software and major equipment purchases. No software should be installed on Trust-owned devices unless approved by the employee's direct supervisor and the IT department. The Trust installs only properly authorized and licensed software and prohibits any installation or use of unauthorized, unlicensed or illegally-copied software.

Change Management: To protect from changes that could compromise the Trust's operations, the IT department will enforce standards for the approval and deployment of changes to the Trust's IT infrastructure and environment, as well as the implementation of any new applications of any type. These standards require, amongst other provisions, that all changes be appropriately governed and managed – and must be tested, documented, with cyber, business, technical and legal risk areas considered, and have user acceptance documented before being installed in the production environment. The approved deployment plan must include rollback and contingency procedures.

Viruses and Malware: To defend against computer viruses and malware, all computers and devices connecting to the Trust's IT infrastructure must be approved devices and have standard, authorized anti-virus and malware protection software installed. It is the responsibility of the IT department to keep this software updated and of users to report to the IT department any sign of infection. To further enhance security, personal e-mail is not to be accessed on Trust laptops or computers.

Remote Access: Users should assume that remote and/or free public networks, including but not limited to those found in cafes, airports and hotels, are unsecure. Users should avoid, if practicable, accessing confidential information while using public or remote networks that are not secure. This could include, but is not limited to, accessing banking information, personal information of employees or contractors, government filings etc. Users should adhere to this policy in order to prevent interceptions, eavesdropping, unauthorized access or direct attacks that could risk the integrity of the Trust's network.

Lost Devices: To prevent the disclosure of confidential information in lost or stolen devices, the IT department will implement encryption and other security mechanisms to dynamically protect the Trust's data. Users are responsible to take appropriate precautions to prevent damage to, loss or theft of any device issued to them or approved for use by them. Each employee must report immediately to their supervisor and to the IT department any lost or stolen devices and any suspected or confirmed breaches of such devices. The IT department will take the required measures to wipe remotely, where possible, any Trust data still hosted on the lost device. If a user's device is lost, stolen or upon termination, the IT department will wipe the device, which may include user's private information. It is not the responsibility of the Trust to recover any personal data or media from a lost or stolen device.

Equipment: Users are responsible for the hardware assigned to them. Relocations and transfers of equipment must be approved by the IT department.

VPN: In order to protect Trust data while using public networks, the IT department, where required, will provide and support secured remote access, including Virtual Private Networks ("**VPN**"). Only Trust-issued devices will be configured with VPN (or equivalent) access. Users with VPN credentials are responsible for maintaining their confidentiality according to the password provisions of this policy.

Incident Management: To promptly respond to threats, users are expected to communicate information security incidents to the IT department. Security incidents include any violation of this policy that compromises Trust data independently of ownership of the device. The IT department is responsible for the channels and procedures that guarantee that security incidents are identified, contained, investigated and remedied.

F. Legal and Compliance

The Trust will regularly assess cyber security-related developments in order to ensure the implementation of policies related to:

- Cyber security management.
- Management of third party access to Trust networks.
- Other policies as required to ensure minimum standards of care are taken by the organization to protect against cyber threat.

Cyber risk will be monitored through internal audit programs and will be included in a report communicated to the Board of Trustees at least quarterly.

All material contracts should be reviewed by legal counsel as a matter of course and to ensure that the potential cyber risk assumed or created as a result is understood by management.

All contracts for the provision of cyber-related services to the Trust should be reviewed by legal counsel to ensure that management has the understanding of residual risks for purposes of making relevant business decisions.

4. APPROVAL

Approved by the Board of Trustees on August 26, 2022