Reference	EOP/ESG/CSP/01 Version: June 2, 2021
Document Title	Cyber Security Policy ("**Cyber Security Policy**")
Entity	Embassy Office Parks Management Services Private Limited ("**Manager**") in its capacity as the Manager of Embassy Office Parks REIT ("**Embassy REIT**")
Responsibility	Head- Information Technology

Revision History		
Version #	**Version Date**	**Change Type**
V1	June 2, 2021	Created

Document Review Cycle			
#	**Effective Date**	**Next review date**	**Policy Owner**
1	June 2, 2021	Q4 Board Meeting date of the Manager of every Financial Year	Head- Information Technology

Applicability	This policy is applicable to the Manager, Embassy REIT, its special purpose vehicles ("**SPVs**") and its holding company(ies) ("**Holdco**"), collectively referred to as "**Embassy REIT Entities**", and individually as a "**Embassy REIT Entity**" in this document. The Cyber Security Policy provides an integrated set of protection measures that must be uniformly applied across Embassy REIT Entities to ensure a secured operating environment for its business operations. The availability, integrity and confidentiality of information are essential in building and maintaining our competitive edge, cash flow, profitability, legal compliance, and respected company image. This Cyber Security Policy addresses the information security requirements of: **Confidentiality**: Protecting sensitive information from disclosure to Unauthorised individuals or systems. **Integrity**: Safeguarding the accuracy, completeness, and timeliness of information. **Availability**: Ensuring that information and vital services are accessible to authorised users when required Other principles and security requirements such as Authenticity, Non-repudiation, Identification, Authorisation, Accountability and audit ability is also addressed in this policy. This policy applies to all Company employees, directors, consultants, interns, contract workers, associates, and temporary employees.

	Third party service providers providing hosting services or wherein data is held outside Embassy premises, shall also comply with this policy. Scope of this Cyber Security Policy is the information stored, communicated, and processed within Embassy and Embassy's data across outsourced locations.
Background to the Policy	The purpose of this policy is to: i. protect Embassy data and infrastructure, ii. outline the protocols and guidelines that govern cyber security measures, iii. define the rules for company and personal use, and iv. list the company's disciplinary process for policy violations. To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy. To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people). This policy provides a framework and a set of guidelines spelling out acceptable practices and procedures, that minimize the vulnerability of company data, networks and infrastructures to accidental or malicious attacks, with which the stakeholders must comply to protect the confidentiality, integrity, availability, and authenticity of the information.
Responsibility for Compliance	The Head- Information Technology is responsible for maintaining compliance to this policy and procedures thereunder. Any queries regarding the implementation of this policy shall be directed to the Information Technology department. The Company's Cyber Security program will be overseen by individuals with significant authority and independence. The Company has established IT Security Committee This policy shall be reviewed for updates by IT Security Committee on an annual basis. Additionally, this policy may be updated in-line with any recommendations provided by internal/ external auditors.
Definitions	**User** refers to any individual granted credentials to access the company's Information Technology Resources. **Firewall** refers to a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. **Cyber Security** refers to Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

	Penetration Testing refers to a simulated cyber-attack against a computer system to check for exploitable vulnerabilities. Basically, a security Testing used to uncover vulnerabilities, threats and risks that an attacker could exploit in software applications, networks or web application. **Vulnerability Assessment** refers to a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed. **Application Security Testing** refers to the process of making applications more resistant to security threats, by identifying security weaknesses and vulnerabilities in source code.
Focus Areas	To reduce the risk of cyber-attacks and improve upon the security posture of critical information infrastructure, Embassy shall implement following measures.
Information Security Point of contact	Identify a member of senior management, as CISO knowledgeable information security & related issues and designated as a Point of contact, responsible for coordinating security policy compliance efforts and to regularly interact with Department of Information Technology (DIT), which is the nodal agency for coordinating all actions pertaining to cyber security.
Access Management	**Access to the Network** All devices on the network of Embassy should not be accessible without proper Authentication (Preferably Biometric Authentication for Physical access to Computer / Data Centre at Office Premises). **Access to Internet and Intranet** i. Users should not undertake any activity through any website or applications to bypass filtering / Policy / Firewall / Unified Threat Management of the network or perform any other unlawful acts which may affect the network's performance or security. ii. Users are not allowed to change the Network Interface Card configuration, IP address or any other parameters set for accessing company's LAN & WAN without permission of implementing authority. iii. Users shall not connect any other devices to access Internet / any other network in the same client system configured for connecting to LAN/WAN of the company without permission.
Information Security Plan and Procedures	The company shall continuously evolve the security plan in accordance to the changing dynamics & as well as based on the various assessments/audits that are conducted for prevention of cyber-crimes/attacks and prevention of /management of data breaches.
Reporting Security Weaknesses	Users of Embassy Information Technology resources will be required to note and report any observed or suspected security weaknesses or threats to the appropriate manager/ supervisor or the IT Department, via IT service help desk. They must report these weaknesses at the earliest.

	Users must not attempt under any circumstances to prove a suspected weakness. This is for their own protection, as testing weaknesses could be perceived as a potential misuse of the system. Procedures must be established for reporting security software malfunctions. The following should be considered: i. The symptoms of the problem and any messages appearing on the screen should be noted. ii. The computer must be isolated, if possible, and use of it stopped until the problem has been resolved. iii. The matter should be reported immediately to the IT Department via IT service help desk, for appropriate investigation.
Security Incident Management Process	A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality, and authority of data owned by Embassy. <u>Security Incident Plan</u> The Embassy incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise including notification of relevant external partners. Specific areas covered in the plan include: i. Specific incident response procedures. ii. Business recovery and continuity procedures. iii. Data backup processes. iv. Analysis of legal requirements for reporting compromises. v. Identification and coverage for all critical system components. vi. Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers. At least once every year, the Information Technology Department must utilize simulated incidents to mobilize and test. Implementing Department reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the Implementing authority. Any security incident noticed must immediately be brought to the notice of relevant authority and the Implementing Department. <u>Security Response Team</u> **Security Response Team** - Information Technology Department management must organize and maintain a designated security response team (SRT) that will provide accelerated problem notification, damage control, and problem correction services in the event of computer related emergencies such as virus infestations and hacker break-ins. A member of the Information Security Department is notified of any emergencies or incidents. **Computer Incident Response Team Availability** - Embassy Computer Emergency Response Team must be available at all times to respond to alerts that include but are not limited to evidence of unauthorized activity, detection of unauthorized wireless

	access points, critical IDS alerts, and reports of unauthorized critical system or content file changes. **Testing the Computer Emergency Response Team** - At least once per year, the Information Security Department must utilize simulated incidents to mobilize and test the adequacy of the Embassy Computer Emergency Response Team.
Information Security Risk Assessment	The company shall carry out periodic IT security risk assessments and determine acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievement of organizational goals/objectives. The company shall perform this test twice a year and evaluate the adequacy and effectiveness of technical security control measures implemented for IT systems and networks. Especially, also, test and evaluate is necessary after each significant change to the IT applications/systems/networks and can include, as appropriate the following: i. Penetration Testing ii. Vulnerability Assessment iii. Application Security Testing iv. Web Security Testing
Information Security Audit	The company shall conduct information Security audits to check compliance against Policies and procedures on an annual basis and when there is major upgradation/change in the Information Technology Infrastructure, by an independent IT Security Auditing organization.
Creating Cyber Security Awareness	Apart from providing regular advisory through various communication channels, an information security awareness program will be conducted to address security education for Embassy employees. The awareness program will review Cyber Security Policy, threats and concerns, and the proper use of information processing facilities (e.g., logon procedures and use of software packages) to minimize possible security risks. The program will additionally include the procedure to follow to report incidents (security breach, threat, weakness, or malfunction) that might have an impact on the security of Embassy information.
Amendment	This policy will stand automatically amended to the extent of any relevant change(s) in the applicable law and or for any change(s) in fact.