Policy on Cyber Security and Data Privacy

NEXUS SELECT

Introduction

Nexus Select Mall Management Pvt. Ltd. (Nexus Select) is the Indian retail portfolio arm of world's leading investment firm, The Blackstone Group. This policy defines the mandatory Cyber Security requirements for Nexus Select and its Portfolio Entities, Any entity may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy. This Policy is an Extension of Information Security Policy in IT Policy.

This policy is inspired by expectations of Global Reporting Initiative, S&P Global Corporate Sustainability Assessment and GRESB

Objective

a) NexusIT takes Cyber Security best practice suggestion from Revantage Asia Team, few implementations already done like - Windows Spectre Built, Intune and Mobile Application Management.

b) Few tools are used as Cyber tools, - KnowBe4 Phishing and Training Module.

c) Nexus will follow Governance Document shared by Revantage Asia team.

d) This policy acts as an umbrella document of IT security policy and associated standards. This policy defines the responsibility to:

➢ Protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets.

➢ Manage the risk of security exposure or compromise.

➢ Assure a secure platform

➢ Stable information technology (IT) environment.

➢ Identify and respond to events involving information asset misuse, loss or unauthorized disclosure.
➢ Patch Management, Server Security, Social Engineering Awareness, Anti-Virus, Incident Handling, IT disposal, Communication Equipment Policy etc.

➢ Monitor systems for anomalies that might indicate compromise, data breach response and ➢ Promote and increase the awareness of information security.

➢ Failure to secure and protect the confidentiality, integrity, and availability of information assets in today’s highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions, and vital government functions; compromise data; and result in legal and regulatory non-compliance.

➢ This policy benefits entities by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity, and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures and practices and know how to protect information.

Scope

This policy encompasses all systems, automated and manual, for which the entity has administrative responsibility, including systems managed or hosted by third parties on behalf of the entity. It addresses all information, regardless of the form or format, which is created or used in support of business activities

Policy Statements

Organizational Security:

- Nexus Select shall designate an individual or group to be responsible for the asset function assuring that: Risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise with regard to the overall strategic goals and objectives of carrying out its core missions and business functions; and the management of information assets and information system-related security risks is consistent, reflects the risk tolerance, and is considered along with other types of risks, to ensure mission/business success
- Nexus Select can designate an individual or group to be responsible for the technical information security function. For purposes of clarity and readability, this policy will refer to the individual, or group entity representative. This function will be responsible for evaluating and advising on information security risks. Although the technical information security function may be outsourced to third parties, each entity retains overall responsibility for the security of the information that it owns.

Functional Responsibilities:

IT Manager/ IT Lead/ IT Head is responsible for:

- Evaluating and accepting risk on behalf of the entity.
- Identifying information security responsibilities and goals and integrating them into relevant processes
- Supporting the consistent implementation of information security policies and standards
- Supporting security through clear direction and demonstrated commitment of appropriate resources.
- Implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization
- Determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the dat
- Promoting awareness of information security best practices through the regular dissemination of materials provided by the designated security representative
- Participating in the response to security incidents.
- complying with notification requirements in the event of a breach of private information.
- Adhering to specific legal and regulatory requirements related to information security, promoting information security awareness
- communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

Informational Technology Team is Responsible for:

- Supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners
- Providing resources needed to maintain a level of information security control consistent with this policy
- Identifying and implementing all processes, policies, and controls relative to security requirements defined by the business and this policy
- Implementing the proper controls for information owned based on the classification designations.
- Providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);
- Fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures

The workforce is responsible for:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted.
- Protecting information and resources from unauthorized use or disclosure.
- Protecting personal, private, sensitive information from unauthorized use or disclosure
- Abiding by Acceptable Use of Information Technology Policy
- Reporting suspected information security incidents or weaknesses to the appropriate manager and designated security representative

Separation of Duties:

- To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.
- Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and Vulnerability Assessment, Patch management.
- The audit and approval of security controls must always remain independent and segregated from the implementation of security controls.

Social Engineering Awareness Policy:

The Social Engineering Awareness bundle is a collection of policies and guidelines for employees of Nexus Group. This Employee Front Desk Communication Policy is part of the Social Engineering Awareness.

To protect Nexus assets, all employees need to defend the integrity and confidentiality of Nexus resources.

To make employees aware that (a) fraudulent social engineering attacks occur, and (b) there are procedures that employees can use to detect attacks.

- Employees are made aware of techniques used for such attacks, and they are given standard procedures to respond to attacks.

- Employees know who to contact in these circumstances.
- Employees recognize they are an important part of Nexus security. The integrity of an employee is the best line of defence for protecting sensitive information regarding Nexus resources.

To create specific procedures for employees to follow to help them make the best choice when

- Someone is contacting the employee - via phone, in person, email, fax or online - and elusively trying to collect Nexus sensitive information.
- The employee is being “socially pressured” or “socially encouraged or tricked” into sharing sensitive data.

Sensitive information of Nexus will not be shared with an unauthorized individual if he/she uses words and/ or techniques such as the following:

- An “urgent matter”
- A “forgotten password”
- A “computer virus emergency”
- Any form of intimidation from “higher level management”
- Any “name dropping” by the individual which gives the appearance that it is coming from legitimate and authorized personnel.
- The requester requires release of information that will reveal passwords, model, serial number, or brand or quantity of Nexus resources.
- The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person.
- The techniques are used by a person that declares to be "affiliated" with Nexus such as a sub-contractor.
- The techniques are used by an individual that says he/she is a reporter for a well-known press editor or TV or radio company.
- The requester is using ego and vanity seducing methods, for example, rewarding the front desk employee with compliments about his/her intelligence, capabilities, or making inappropriate greetings (coming from a stranger).

Action:

- All employees MUST attend the security awareness training within 90 days from the date of employment and every year thereafter using KnowBe4 Tool, including PAB training via KnowBe4 (mandatory)
- If any suspicious issue is detected by a employee, then the identity of the requester MUST be verified before continuing the conversation or replying to email, fax, or online.
- If the identity of the requester described in Policy Compliance below CANNOT be promptly verified, the person MUST immediately contact his/her supervisor or direct manager.
- If the supervisor or manager is not available, that person MUST contact the security personnel or IT Support Desk, or IT Cyber Support Desk.
- If the security personnel are not available, the person described in section 3.0 MUST immediately drop the conversation, email, online chat with the requester, and report the episode to his/her supervisor before the end of the business day.

Enforcement:

- An employee found to have violated this policy may be subject to disciplinary action.

Account Management Access Control Policy:

The purpose of this standard is to establish the rules and processes for creating, maintaining, and controlling the access of a digital identity to an entity's applications and resources for means of protecting their systems and information.

This standard covers all systems developed by, or on behalf of the entity, that require authenticated access. This includes a ll development, test, quality assurance, production and other ad hoc systems.

Account management and access control includes the process of requesting, creating, issuing, modifying and disabling user accounts; enabling and disabling access to resources and applications; establishing conditions for group and role membership; tracking accounts and their respective access authorizations; and managing these functions.

Account Management Roles:

Account management and access control require that the roles of Information Owner, Account Manager and, optionally, Account Administrator and Entitlement Administrator, are defined and assigned for each resource and application.

A listing of authorized users in these roles must be documented and maintained. The associated tasks and responsibilities for each role are described below. Each role may belong to one or more individuals depending on the application. In some cases, a single individual or group may be assigned more than one of these roles

a. Information Owner

Information owners are people at the managerial level within an entity who:

- Delegate account managers to ensure the appropriate level of information access is provided. Delegation can be to individual users, groups and/or third parties (e.g., another entity).
- Define roles and groups, as well as the corresponding level of access to resources for that role or group.
- Determining who should have access.
- Determine the identity assurance level for the application and/or data.
- Review that accounts and access controls are commensurate with overall business function and that the associated rights have been properly assigned, at a minimum, annually.
- Require business units with access to protected resources to notify account managers when accounts are no longer required, such as when users are terminated or transferred and when individual access requirements change.

b. Account Manager

Account managers maintain accounts. They are the delegated custodians of protected data. Account managers

- Maintain appropriate levels of communication with the information owners to determine the level or degree of access granted to an individual.
- Determine the technical specifications needed to set access privileges.
- Delegate account management functions to account administrators.
- Create and maintain procedures used in managing accounts.
- Perform all account administrator duties as required.

c. Account Administrators

Account administrators are an optional subset of the account manager role. They do not determine procedures. System rights and/or responsibilities are assigned to them by the account manager.

All account administrator responsibilities are contained within the role of account manager should an account administrator not exist. A subset of account administrator duties may be assigned as appropriate.

For example, a role for password reset only may exist for service desk employees. Additionally, some of these responsibilities may remain with the account manager should that manager determine it is necessary. For account management, the administrator may:

- Maintain any necessary information supporting account administration activities, including account management requests and approvals.
- Enrol new users.
- Enable/disable user accounts.
- Create and maintain user roles and groups.
- Assign rights and privileges to a user or group.
- Collect data to periodically review user accounts and their associated rights.
- Assign new authentication tokens (e.g., password resets)

d. Entitlement Administrators:

Entitlement administrators are an optional subset of the account manager role. Rights and/or responsibilities are assigned to them by the information owner and generally include:

- Assign rights and privileges to a user or group.
- Collect data to periodically review user accounts and their associated rights.
- Maintain any necessary information supporting account administration activities including account management requests and approvals.

Account Types:

Account types include Individual, Privileged, Service, Shared, Default Non-Privileged (e.g., Guest, Anonymous), Emergency, and Temporary. All account types must adhere to all applicable rules as defined in the Authentication Tokens Standard.

a. Individual Accounts:

Individual Accounts: An individual account is a unique account issued to a single user. The account enables the user to authenticate to systems with a digital identity. After a user is authenticated, the user is authorized or denied access to the system based on the permissions that are assigned directly or indirectly to that user.

Note: All Nexus IT Team engineer at Mall will get Global Admin READ access ONLY, On Demand with email approval from AGM IT Infra and Security or IT Head, Intune Admin will be given.

b. Privileged Accounts:

A privileged account is an account which provides increased access and requires additional authorization. Examples include a network, system or security administrator account. A privileged

account may only be provided to members of the workforce whom require it to accomplish their job duties. The use of privileged accounts must be compliant with the principle of least privilege. Access will be restricted to only those programs or processes specifically needed to perform authorized business tasks and no more. There are two privileged account types - Administrative Accounts and Default Accounts.

1. Administrative Accounts: Accounts given to a user that allow the right to modify the operating system or platform settings, or those which allow modifications to other accounts. These accounts must
   - be at an Identity Assurance Level commensurate with the protected resources to which they access.
   - not have user-IDs that give any indication of the user's privilege level, e.g., supervisor, manager, administrator, or any flavour thereof.
   - be internally identifiable as an administrative account per a standardized naming convention.
   - be revoked in accordance with organizational requirements

* IT Consultant from Sonata and QA Team (MVW) will also get Global Admin Access on M365 portal

2. Default Privileged Accounts: Default privileged accounts (e.g., root, Administrator) are provided with a particular system and cannot be removed without affecting the functionality of the system.

Default privileged accounts must:

- Be disabled if not in use or renamed if technically possible.
- Only be used for the initial system installation or as a service account. When technically feasible, alerts must be issued to the appropriate personnel when there is an attempt to log-in with the account for access.
- Not use the initial default password provided with the system.
- Have password known or accessible by at least two individuals within the SE, if password is known by anyone. As such, restrictions for shared accounts, outlined below, must be followed.

2. Service Accounts: A service account is not intended to be given to a user but is provided for a process. It is to be used in situations such as to allow a system to run jobs and services independent of user interaction. Service accounts must:

- Have an assigned owner responsible for documenting and managing the account.
- Be restricted to specific devices and hours when possible.
- Never be used interactively by a user for any purpose other than the initial system installation or if absolutely required for system troubleshooting or maintenance. Wherever technically feasible, administrators should leverage "switch user" (SU) or "run as" for executing processes as service accounts.
- Never be for any purpose beyond their initial scope.
- Be internally identifiable as a service account per a standardized naming convention, where possible.
- Not allow its password to be reset according to any standardized and/or forced schedule. However, should an employee with knowledge of said password leave the entity, that password must be changed immediately.

- Have password known or accessible by at least two individuals within the entity, if password is known by anyone. As such, restrictions for shared accounts, outlined below, must be followed.

Shared Accounts:

A shared account is any account where more than one person knows the password and/or uses the same authentication token. Use of shared accounts is only allowed when there is a system or business limitation preventing use of individual accounts. These cases must be documented by the information owner and reviewed by the IT Security/designated security representative. Additional compensatory controls must be implemented to confirm accountability is maintained. Shared accounts must:

- Have the tokens(e.g. password) reset when any of its users no longer needs access, or otherwise in accordance with the Authentication Tokens Standard.
- Be restricted to specific devices and hours when possible.
- Wherever technically feasible, have its users log on to the system with their individual accounts and "switch user" (SU) or "run as" the shared account.
- Have strictly limited permissions and access only to the system(s) required.
- MFA should be configured while using Shared Account

Default Non-Privileged Accounts:

The default non-privileged account (guest or anonymous user) is an account for people who do not have individual accounts. An example of where this might be necessary is on a public Wi-Fi network. This account type must:

- Be disabled until necessary.
- Have limited rights and permissions.
- Only be allowed after a risk assessment
- Have compensatory controls that include restricted network access.
- Be assigned a password that the user cannot change but that is changed monthly, at a minimum, by an administrator.
- Not allow the account to be assigned for delegation by another account.
- Have a log maintained of users to whom the password is given.

Emergency Accounts:

Emergency Accounts are intended for short-term use and include restrictions on creation, point of origin, and usage (i.e., time of day, day of week). System engineers may establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency accounts must be automatically disabled after 24 hours.

Temporary Accounts:

Temporary accounts are intended for short-term use and include restrictions on creation, point of origin, usage (i.e., time of day, day of week), and must have start and stop dates. An entity may establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation, such as for vendors, manufacturers, etc. These accounts must have strictly limited permissions and access only to the systems required.

Account Management and Access Control Functions:

Automated mechanisms must be employed to monitor the use and management of accounts. These mechanisms must allow for usage monitoring and notification of atypical account usage. Thresholds for alerting should be set based on the criticality of the system or assurance level of the account.

Staff in the appropriate account management/access control role(s) must be notified when account management activities occur, such as, accounts are no longer required, users are terminated or transferred, or system usage or need-to-know changes. This should be automated where technically possible.

Automated access control policies that enforce approved authorizations for information and system resources must be in place within systems. These access control polices could be identity, role or attribute based.

By default, no one has access unless authorized.

The Identity Assurance Level (IAL) of a system determines the degree of certainty required when proofing the identity of a user. The following table describes the level of confidence associated with each IAL

Identity Assurance Level:

Description

1 Low or no confidence in the asserted identity's validity

2 Confidence in the asserted identity's validity

3 High confidence in the asserted identity's validity

Table: Account Management Standards per Identity Assurance Level which describes the level.

	Identity Assurance Levels		
Category	1	2	3
Account disabled automatically after *x* days of inactivity	1096	90	90
Send notification *x* days before account disabled	30	30	14
Account locked after *x* number of consecutive failed login attempts	10	5	3
Account creation requires an authoritative attribute that ties the user to their account. For example, this could be an employee ID, driver's license ID, tax ID, or unique individual email address.	No	Yes	Yes
Email notification will be sent to the user for the following events: • Token change (password, pre-registered knowledge token, out of band (OOB) token information) • Account disabled due to invalid attempts • Forgotten User Identification (UID) issued • Account attribute change (e.g., name change) • Account re-activation	If known	Yes	Yes
Self-service functionality allowed	Yes	Yes	No

For all Assurance Levels, the following must be adhered to:

a. Creating New Accounts:

To create an account, there must be a valid access authorization based on an approved business justification and a request must be made to create the account.

b. Modifying Account Attributes (i.e., changing users' names, demographics, etc.):

Modifications must only be made by the authenticated user or an authorized account manager.

c. Enabling Access: Access is granted, based on the principle of least privilege, with a valid access authorization

d. Modifying Access: Access modifications must include a valid authorization. When there is a position change (not including separation), access is immediately reviewed and removed when no longer needed.

e. Disabling Accounts/Removing Access:

- Event/Risk Based (Administrative Disable): When an account poses or has the potential to pose a significant risk, either the account is disabled and/or access attributes are removed upon discovery of the risk. Close coordination between the information owners, account managers/administrators, legal, incident response stakeholders and human resource managers is essential in order for timely execution of removing or restricting user access. Significant risk may include a disgruntled employee, or one who has been identified by as a potential risk. Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations. An account identifier is required to identify these accounts and prevent inappropriate re-enabling of the account/access. Re-enabling the account requires explicit approval of the entity, Self-service mechanisms may not be used to re-enable the account.
- De-provisioning Upon Separation: All user accounts (including privileged) must be disabled immediately upon separation. In addition, credentials must be revoked in accordance with organizational requirements, and access attributes must be removed. Self-service mechanisms may not be used to re-enable the account. Account might be kept active with auto forward, but password and OTP (MFA) will be changed.
- Inactivity Disable: When an account is disabled due to inactivity, access attributes may remain unchanged if deemed appropriate by the information owner.

f. Reviewing Accounts and Access:

- Information owners must review all accounts on an annual basis (minimally) to determine if they are still needed.
- Access to privileged accounts must be reviewed every six months (minimally) to determine whether or not they are still needed.
- Information owners must review account authorizations and/or user access assignments on an annual basis (minimally) to determine if all access is still needed.

- Accounts or records of the account must be archived after 5 years of inactivity or after specific audit purposes are met, if applicable for Nexus and its Auditors, otherwise this is not applicable.

g. Unlocking User Accounts: In order for an administrator or user support agent to unlock an account for a user, the user must be vetted through pre-registered knowledge tokens as per the Authentication Tokens Standard.

h. Secure Log on Procedures: Where technically feasible, access must be controlled by secure log-on procedures as follows:

- Must not display tokens (e.g., password, PIN) being entered.
- Must display the following information on completion of a successful log-on: i. Date and time of the previous successful log-on; and ii. Details of any unsuccessful log-on attempts since the last successful log-on.

i. Session Inactivity Lock: Sessions must be locked after a maximum inactivity period of 15 minutes or whatever is available in tool or Revantage Asia Governance Document. Session inactivity locks are temporary actions taken when users stop work and move away from their immediate vicinity but do not want to log out because of the temporary nature of their absences. Users must re-authenticate to unlock the session.

j. Connection Time Out

- Sessions must be automatically terminated after 18 hours or after “pre-defined” conditions such as targeted responses to certain types of incidents this can be changed if mentioned in Revantage Asia Governance Policy or as per business needs.

k. Logging/Auditing/Monitoring:

- All account activity must be logged and audited in accordance with the Security Logging Standard. The ability to modify or delete audit records must be limited to a subset of privileged accounts. Any modification to access attributes must be recorded and traceable to a single individual.

Enforcement:

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time. If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the AGM IT Infra and Security/ IT Head exception process:

Data Breach Response Policy:

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Nexus IT Team intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches (refer IT Nexus Policy) and how Nexus established culture of openness, trust and integrity should respond to such activity. Nexus IT Team is committed to protecting Nexus employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly

This policy mandates that any individual who suspects that a theft, breach or exposure of Nexus Protected data or Sensitive data has occurred must immediately provide a description of what occurred via e-mail to Nexus IT Team. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information of Nexus members. Any agreements with vendors will contain language similar that protects the fund.

Policy Confirmed theft, data breach or exposure of Nexus Group Protected data or Sensitive data

As soon as a theft, data breach or exposure containing Nexus Protected data or Sensitive data is identified, the process of removing all access to that resource will begin.

The corporate IT Head will chair an incident response team to handle the breach or exposure. The team will include members from:

- IT Infrastructure
- IT Applications
- Finance (if applicable)
- Legal (if applicable)
- Member Services (if Member data is affected)
- Human Resources (if applicable)

The affected unit or department that uses the involved system or output or whose data may have been breached or exposed

Additional departments based on the data type involved, Additional individuals as deemed necessary by the IT Manager Confirmed theft, breach or exposure of Nexus data.

The IT Manager/ IT Head will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyse the breach or exposure to determine the root cause

Develop a communication Plan

Work with Nexus IT Team, legal and human resource departments to decide how to communicate the breach to a) internal employees, b) the public, and c) those directly affected.

Ownership and Responsibilities

- Sponsors are those members of the Nexus Group that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any Nexus Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Information Security Administrator is that member of the Nexus Group, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides

administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors

- Users include virtually all members of the Nexus Group to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by Head IT (in absence of Head IT, AGM IT will take over) and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources – all additional attendees are optional.

Enforcement:

An employee found to have violated this policy may be subject to disciplinary action. Any third-party partner company found in violation may have their network connection terminate which also might lead to cancellation of services.

Password Policy:

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Nexus and its Entities corporate network. As such, all Nexus employees (including contractors and vendors with access to Nexus systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

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.

The scope of this policy includes all personnel 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 Nexus facility, has access to the Nexus network, or stores any non -public Nexus information:

- All system-level passwords (e.g., Root, Admin, Windows admin, application administration accounts, Network SSID, Firewall Admin etc.) must be changed on at least once on quarterly basis as a best practice
- All production system-level passwords must adhere to Information Security Password Best Practices.
- Password should be minimum 8 or above characters
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 6 months. The recommended change interval is every 3 months (90 days).
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used for network management, the community strings must be defined as something other than the standard defaults of “public,” “private” and “system” and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below:

Guidelines:

A. General Password Construction Guidelines

Passwords are used for various purposes at Nexus. Some of the more common uses include user level accounts, web accounts, email accounts, screen saver protection, Email password, and local router logins. Since a very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

• The password contains less than eight characters.

• The password is a word found in a dictionary (English or foreign).

• The password is a common usage word such as:

o Names of family, pets, friends, co-workers, fantasy characters, etc.

o Computer terms and names, commands,sites, companies, hardware, software.

o The words “WRPL”, “Local of Mall”, “Nexus Group” or any derivation.

o Birthdays and other personal information such as addresses and phone numbers.

o Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321,Nexus@123, Passw0rd, Password@123, Login@123 etc.

o Any of the above spelled backwards.

o Any of the above preceded or followed by a digit (e.g., secret1,1secret)

B. Strong Passwords have the following characteristics:
   - Contain both upper and lower-case characters (e.g., a-z, A-Z).
   - Have digits and punctuation characters as well as letters e.g., 0-9, !,@#$%^&*()_+|~-=\`{}[]:”;’<>?,./) – if special character is applicable for particular infra or software/ application
   - Are at least eight alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
   - Are not words in any language, slang, dialect, jargon, etc.
   - Are not based on personal information, names of family, Date of Birth, Residence etc.
   - Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: “This May Be One Way To Remember” and the password could be: “TmB1w2R!” or “Tmb1W>r~” or some other variation

NOTE: Do not use either of these examples as passwords!

Enforcement: An employee found to have violated this policy may be subject to disciplinary action.

Patch Management Policy

This Policy is extension of Server Security Policy in IT policy

Security patch management (patch management) is a practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. By applying security related software

or firmware updates (patches) to applicable IT systems, the expected result is reduced time and money spent dealing with exploits by reducing or eliminating the related vulnerability

This standard relates specifically to vulnerabilities that can be addressed by a software or firmware update (patch) and applies to all software used on the Nexus entity's systems. The Vulnerability Scanning Standard should be followed for requirements on addressing non-patched vulnerabilities

Information Statement:

1. IT engineer at Mall will be responsible to implementation of patch management.

2. If patch management is outsourced, service level agreements must be in place that address the requirements of this standard and outline responsibilities for patching. If patching is the responsibility of the third party, entities must verify that the patches have been applied, Ideally OS patching should be done within 45 days to 60 days once.

3. A process must be in place to manage patches. This process must include the following: ·

- Monitoring security sources for vulnerabilities, patch and non-patch remediation, and emerging threats.
- Overseeing patch distribution, including verifying that a change control procedure is being followed.
- Testing for stability and deploying patches(optional)
- Using an automated centralized patch management distribution tool, whenever technically feasible, if applicable, otherwise manual patching can be done if server count is more than 10 (On-premise + Cloud)

a. Maintains a database of patches; (excel will do)
b. Deploys patches to Servers and Firewalls, endpoint patching is done via M365 Intune; and
c. Verifies installation of patches, proper Change Request should be raised and shared after closure with relevant patch installed (before and after screenshot/ artifacts should be shared)

4.A process must be in place to manage patches. This process must include the following: ·

5. As per the Information Security Policy, all entities must maintain an inventory of hardware and software assets. Patch management must incorporate all installed IT assets.

6. Patch management must be prioritized based on the severity of the vulnerability the patch addresses. In most cases, severity ratings are based on the Common Vulnerability Scoring System (CVSS). A CVSS score of 7-10 is considered a high impact vulnerability, a CVSS score of 4-6.9 is considered a moderate impact vulnerability and a CVSS of 0-3.9 is considered a low impact vulnerability.

7. To the extent possible, the patching process must follow the timeline contained in the table below, this is applicable as per server role and availability of server for patch management (with 45days to 60days of OS patch release)

Impact/Severity	Patch Initiated	Patch Completed
High	Within 24 hours of patch release	Within 1 week of patch release
Medium	Within 1 week of patch release	Within 1 month of patch release
Low	Within 1 month of patch release	Within 2 months of patch release, unless IT Team determines this to be an insignificant risk to the environment

8. If patching cannot be completed in the timeframe listed in the table above, compensating controls must be put in place within the timeframes above and the exception process must be followed.

9. If a patch requires a reboot for installation, the reboot must occur within the timeframes outlined above.

Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the IT Head exception process.

10. VAPT Annual Exercise POA

Purpose : VAPT will be performed annual once for Nexus Select and its entities.

Acceptable Encryption Policy:

Adheres to the Nexus IT Policy, also Encryption on corporate computer system should be done via Windows Spectre Built

Key Agreement and Authentication:

- Nexus will encrypt endpoints via BITLOCKER which comes via M365 E5 with Audio Conference License.
- Server, Network Devices are not applicable for encryption

a. Mobile Application Management [M365 Azure Infra]
    - Mobile Application Management will be deployed on all mobile devices which has corporate mailbox installed
    - Complete policy will be deployed as per Revantage Asia Governance Document
b. Sensitivity Label on Corporate Outlook and Microsoft App
    - M365 Sensitivity labels will be deployed 100% on all corporate mailbox
    - Sensitivity Labels will be also installed on Microsoft Apps.
c. Malware Protection Policy (M365 Defender and Firewall)
    - Nexus will protect its endpoints only via M365 Defender and Firewall
    - Central policy is deployed over employees who are using M365 licenses
d. Virtual Private Network Policy
    - Nexus IT Engineers at Mall will get Firewall VPN access to support device from remote.
    - Not all Nexus IT Engineers will get Firewall VPN access only cluster leads of Nexus IT will get access to help and support Firewall Administration
    - Nexus will also give VPN for Firewall on need basis to 3rd Party Firewall Admin for troubleshooting purpose and will disable/ deactivate VPN once activity is completed.
    - Email approvals will be given by NexusIT Designated IT Head/ AGC - IT Infra, Operations and Cyber Security

Reporting

Nexus Select intends to consistently monitor the implementation of this policy. We are committed to establish suitable procedures and infrastructure to meeting this compliance.

Execution and Review

Execute: All the employees shall have the primary responsibility to execute and implement the directives as per this policy.

Review: Information Technology department shall review the implementation of this policy supplement and adopt suitable procedures to support compliance.

This policy shall be reviewed annually to ensure its effective implementation and amendments

Version	Drafted by	Approved by	Effective from
1.0	IT	Chief Technology Officer	1st April 2022
1.1	IT	Chief Technology Officer	20th Sep 2022