UV Asset Reconstruction Company Limited

(UVARCL)

INFORMATION SECURITY AND ACCESS CONTROL POLICY

**Approved by the Board of Directors in its Board meeting held on December 24, 2025.*

INFORMATION SECURITY AND ACCESS CONTROL POLICY

1. Policy Statement

1.1. This is a comprehensive policy document covering standard operating procedures that are implemented and documented as per the requirements of UVARCL.
1.2. Background
1.3. Access controls are necessary to ensure only authorized users / employees can obtain access to UVARCL's systems and information.
1.4. Protecting access to IT systems and applications is critical to maintain the integrity of UVARCL, its technology and client data and prevent unauthorized access to such resources.
1.5. Access to UVARCL systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.
1.6. All information stored on any electronic device used for UVARCL work, including desktops, laptops, mobile devices, cloud platforms and external drives, is considered UVARCL proprietary information and must be protected accordingly.
1.7. Users must immediately report any theft, loss, misuse or unauthorized exposure of systems, devices or information to the IT Team.
1.8 UVARCL systems, networks, applications, and connected devices will be monitored and logged. UVARCL will conduct an annual Information Security and IT audit, including VAPT.

2. Policy Objective

2.1. The objective of this policy is to ensure UVARCL has adequate controls to restrict access to systems and data, and follows a standard protocol with best practices for all clients.
2.2. To ensures secure, ethical and responsible use of UVARCL information resources including internet, email, cloud services, mobile devices and communication systems.
2.3. The policy aims for legal risk management and to prevent misuse, operational disruption or reputational impact due to improper use of the UVARCL IT environment.

3. Scope

This policy applies to:
3.1. All offices.

3.2. All employees, consultants, contractors, agents, and authorized users accessing UVARCL IT systems and applications.

3.3. All IT systems or applications managed by UVARCL that store, process or transmit information, including network and computer hardware, software, applications, mobile devices and telecommunication systems.

3.4. Any personal device (BYOD) used to access UVARCL email, data, systems or networks must comply with all applicable controls defined in this policy.

3.5. All cloud-based services, VPN connections, remote tools used for UVARCL business activity.

4. Definitions

4.1. "Access Control" is the process that limits and controls access to resources of a computer system.
4.2. "Users" includes all employees, consultants, contractors, agents, and authorized users accessing UVARCL IT systems, applications and data.
4.3. "System or Application Accounts" are user IDs created on IT systems or applications associated with specific access privileges.
4.4. "Privileged Accounts" are system or application accounts that have advanced permissions such as administrative or super-user access.
4.5. "Access Privileges" refer to system permissions associated with an account, including permissions to access or change data, process transactions or update settings.
4.6. "Administrator Account" is a user account with advanced privileges necessary for system administration tasks.
4.7. "Application and Service Accounts" are non-personal accounts used by systems, applications or services.
4.8. "Proprietary Information" refers to all data owned or managed by UVARCL stored on any platform or device.
4.9. "Remote Access" refers to any access to UVARCL systems or networks initiated from outside UVARCL premises.
4.10. "Sensitive Data" includes client data, authentication data, financial data and any information where access is restricted.

5. Guiding Principles – General Requirements

5.1. UVARCL will provide access privileges to users (including networks, systems, data, applications, computers and mobile devices) based on the following principles:
5.1.1 Need to know – access granted only to user required to perform assigned responsibilities.
5.1.2 Least privilege – minimum rights required to perform assigned duties.
5.2. Requests for user accounts and access privileges must be formally documented and approved.
5.3. Application and service accounts must only be used by application components.
5.4. User account /Access privilege must be removed immediately when a user leaves UVARCL or no longer requires system access.
5.5. Existing user accounts and access rights will be reviewed at least quarterly to detect dormant accounts or excessive privileges.
5.6. UVARCL systems must be used for UVARCL business activity only and should not be used for personal commercial activity, unauthorized downloading, copyright violations, or accessing inappropriate or offensive content.
5.7. Users must exercise good judgment when using internet, email and communication platforms and avoid activities that may harm UVARCL's reputation.
5.8. Activities that may disrupt systems, introduce malware, bypass authentication, conduct unauthorized scanning or intercept data are strictly prohibited.

6. Access Control Requirements

6.1. All users will be allotted unique ID to access UVARCL systems and applications. Passwords must be set as per the Password Policy.
6.2. Password Policy
6.2.1. All passwords should be of minimum 8 characters and a combination of alphanumeric characters (one upper case, one small case, one numeric and one special).
6.2.2. All passwords will reset after a period of 6 months.
6.2.3. Passwords cannot be reset within 24 hours of creation. In case required to be authorised by HR department.
6.2.4. Password cannot be the same as last 4 passwords.
6.2.5. Passwords with sequential or repeated characters are not allowed.
6.2.6. The system will lock out the user after 10 invalid login attempts.
6.2.7. The system will ask the user to re-login if idle for more than 15 minutes.
6.2.8. At the time of first login, users are advised to change their password.
6.2.9. Passwords must not contain dictionary words, personal information, or easily guessed sequences.
6.2.10. Passwords used for UVARCL systems must not be used for personal accounts.
6.2.11. Passwords must not be written down or stored insecurely.

6.3. System and application sessions must automatically lock after 15 minutes of inactivity.
6.4. Remote access must use secure channels such as VPN with multi-factor authentication.
6.5. Unauthorized hotspots, personal modems or unapproved network connections must not be used in office premises to access UVARCL systems.
6.6. Privileged or administrator access will be assigned only where necessary, recorded, monitored and reviewed.
6.7. Log will be maintained for administrator access and other user access
6.8. User accounts must be disabled after 30 days of inactivity.
6.9. All access changes must follow formal approval.
6.10 Data Handling
6.10.1. Only authorized personnel working on the account/portfolio will have access to data on a need-to-know basis.
6.10.2. All data received whether through email, apps, bank systems etc. must always be treated with strict confidence.
6.10.3. Wherever needed, software such as WinZip or RAR shall be used for encrypting sensitive data before transmission.

7. External media, Firewall and Antivirus Policy, patch management and vulnerability scanning

7.1 Firewall protection to be installed in the system. The firewall to have deny all rule implemented by default and monitor, manage and implement firewall policies on the network.
7.2. Vulnerability scans to be performed on all systems on the domain on regular basis.
7.3. Work related websites can only be assessed by users after approval by authorised person.
7.4. No external media to be accessible from any of the systems in the domain. This includes USB drive, External HDD and Card readers.
7.5. Antivirus Software with active license to be is installed both at the end user desktop/laptop as well as the server level.
7.6. Anti-Virus updates to be downloaded automatically when available and be applied across all machines.
7.7. All systems to be scanned automatically every day and alert generated for any threats that are found.
7.8. SMB & Telnet services must be disabled.
7.9. Firewall must have facility of intrusion detection/prevention systems (IDS/IPS) and to enable or disable IP.
7.10. Vulnerability threats if found/Reported will be remediated as per the following timelines.

- Critical 48 hrs.
- High 30 Days
- Medium 60 Days

8. System Requirements

The following is the minimum system configuration requirement of systems installed/to be installed at UVARCL.

Hardware: Laptop with Intel i5, 4 GB RAM,120GB SSD

Software's (OS / Antivirus): WinPro 10, Office – 365 Business, Quick Heal

8.1. All systems must have USB drives blocked, users cannot connect any external devices, tablets, etc.

8.2. To ensure Windows, MS Office, Anti-Virus & Firewall are licensed versions.

8.3. Anti-Virus software is installed on all the system. Automatic updates are enabled to keep the software current.

8.4. Only the authorized person has privileges to install, delete and update software on the systems.
8.5. Any new installation of system / software / printers is to be approved by HR Head.

9. Risk review and Mitigation

Protection of information, information system, infrastructure and facilities from physical and environmental threats is critical to the well-being of the business. Multiple risk factors exist such as unauthorized physical access, unauthorized access to information processing areas and their supporting infrastructure (communications, power). These must be controlled to prevent, detect, and minimize the effects of unintended access to these areas.

9.1. Physical Security Risk

The physical layout is segregated into perimeter zones. Each zone will have a higher level of access restrictions and access authorization requirements.

9.1.1 Public zone and reception zone. (Limited restrictions – area under overall surveillance e.g. Courier/Mail Delivery/Material Delivery etc.)
9.1.2 Office zone (Limited access – registration with reception required. Visitors be always escorted. Area under overall surveillance e.g. Specific access to employees.)

9.1.3 Restricted access zone (Limited access. Escorted access for visitors. Area under surveillance)

9.2. Physical Entry Controls

• All visitors are required to necessarily register at reception area before entering the premises (non-public area).
• Physical access to the Company's facilities beyond public zone is to be restricted to authorized persons only. Authorization to enter restricted facilities is to be granted only when there is a business or technical reason for the person to enter the premises.
• Access to sensitive or critical information processing facilities outside normal working hours must be specifically authorized and logged.
• Access rights must be updated regularly, based on the criticality of the information system.
• Visitors must be provided supervised and controlled access to secure areas in accordance with the physical access control procedures.
• All physical access records, including Visitor Logs and staff Biometric Log records, must be stored for at least six months. Biometric logs must be reviewed periodically.

Description

Supervised and controlled access includes:

• Every visitor has to Sign the Visitors Log. It must be signed when first entering the company premises. The logbook should record the visitor's name, company, and purpose for visiting to whom visiting, time of entrance, time of departure, date.
• Wearing of a visitor badge to inform personnel that a non-associate is in the area. Those visitors not wearing badges should be challenged for identification.
• The visitors will be escorted by company personnel while the visitor is in the company premises.
• visitors may be asked to declare their belongings like laptop computer, mobile phones, etc. before entering restricted premises.
• Physical access rights must be revoked immediately upon termination/resignation of employees or completion of a consultation or vendor agreement.

9.3. Securing Offices, Telecommunications Closets, Data Center and Facilities

9.3.1 All data centres, equipment rooms, and telecommunications closets must be locked when unattended.
9.3.2 CCTV coverage of the server rooms and critical areas is mandatory.

9.3.3 Only people who are approved to access server rooms and critical areas will have access to them. The access will be restricted through physical locking, biometric lock, access card as necessary.
9.3.4 Network devices such as routers, switches, and hubs must be placed in restricted access zones that provide protection from unauthorized access and all unnecessary ports in network devices be disabled.
9.3.5 Adequate intrusion detection controls (e.g. burglar alarm etc.), and safety devices (e.g. fire alarm, smoke detector, water detection system, close circuit televisions etc.)-to be placed in all office locations, switch rooms and data canters.
9.3.6 Support functions and equipment's such as photocopiers and fax machines should be protected from unauthorized access.

9.4. Equipment Security Risk

9.4.1 Equipment must be placed in a location commensurate with its criticality and its classification.
9.4.2 Equipment must be protected from threats and unauthorized access.
9.4.3 All equipment have AMC plans and/or insurance based on the value of the equipment.
9.4.4 Equipment must not be moved from its location unless authorized by the equipment owner and, if information assets are involved, by the Directors/Management of UVARCL.

9.5. Human Resource Risk

9.5.1 All employees at the time of onboarding have to submit their last three months' salary slip and bank statement as a check of their financial health. Clients are free to do a credit bureau check on employees when needed.
9.5.2 All employees will be provided with adequate and relevant training periodically. This can be information security training, Anti money laundering, etc.
9.5.3 Employees are not supposed to share any work-related information like customer details, login details, password etc among themselves.
9.5.4 Any digression from the above will be viewed strictly and will result in disciplinary action or even termination of the employee.
9.5.5 On resignation or termination, the same will be informed to the client within 24 hours. All logical and physical access privileges will be revoked within 24 hours of the employees' last day.

10. Risk Assessments and Reviews

10.1.1 Information Technology and Infrastructure. Security risk assessment will be done, through reputed vendor, on annual basis and Risk assessment report will be placed before WTD for review and approval. The risk assessment report shall Identify risks if any (internal and external). The same has to be documented. IT team will ensure that rectification of all the observations is done within defined timeline. Final VAPT report to be submitted by vendor after all the rectifications are carried out.

Hardware, Systems and critical support Infrastructure: All systems will be checked with the intent to find vulnerabilities if any either in physical access or network access. The IT team VAPT tests will be conducted by IT team /reputed vendor with due approval of WTD of UVARCL and prior information to client.

11. AWS Cloud Security & Access Management

11.1 All AWS access must follow Identity and Access Management (IAM) principles including least privilege, role-based access assignment and formal authorization.

11.2 AWS access controls must include:
- Identity-based access
- Resource-based access
- Access Control Lists (ACLs)/Control network level access.
- Session access /temporary elevation need based access

11.3 Multi-factor authentication (MFA) must be enabled for all IAM users.
11.4 The AWS root account must only be used for emergency purposes and not as a routine.
11.5 Temporary elevated AWS access must be documented, approved, monitored and revoked immediately after task completion.
11.6 AWS CloudTrail, VPC Flow Logs and CloudWatch logs must be enabled, retained and monitored for anomalies or unauthorized actions.
11.7 AWS resources such as S3 buckets, EC2 instances, RDS databases and other services must be configured to prevent public access unless explicitly approved.
11.8 AWS password should be as per password policy.
11.9 All AWS configuration changes must follow formal change management with documentation and approval.
11.10 Public sharing of AWS resources or files is prohibited without explicit approval.

12. Records Retention and Asset disposal

• All equipment containing storage media (e.g., fixed hard drives) must be checked to ensure that all the critical business information/Data/Applications/licensed software are removed, securely overwritten or destroyed prior to disposal of storage media.
• Any change / discontinuation of software like antivirus / Firewall / Tally / that are used for business purposes need approval by WTD as per change management. There should be business justification for change / upgradation that is suggested.
• Any systems / server / switches that have come to their end of usable life will be replaced by new systems as per change management process.
• All such discarded systems will be first checked and all data residing on such systems will be deleted and the entire system formatted, post which disposal. / Scrapping to happen.
• All such instances of removal of any hardware / software has to be intimated and approved by HR Department beforehand.

13. Approval

13.1. Administrator account will be assigned to all/any of the Whole-Time Directors, HR Head and VP. User access will be given by / after approval of any of the administrator account holders. All access logs will be maintained in the system

14. Amendment to the policy

The Board may review or amend this Policy, in whole or in part, from time to time, as and when required.