Access Control Policy

Introduction

User access to Interr Security information systems shall be granted on the basis of the need-to-know least principle. Users shall be given access only at the appropriate level required to perform their job functions.

Business Requirements for Access Control

All Head Office employees shall be issued a Key card that will grant them access to the main entrance of the office. This shall be subject to a key card reader unlocking the door initially to enable access. Upon loss of a key card, this shall all be reported to the HR Manager as soon as possible to enable it to be de-activated in a timely manner.

User Access Management

User access management shall ensure authorised user access and prevent unauthorised access to information and information systems. This is managed by the IT & System Administrator.

All user access control is managed through system privileges. The Systems and Project Manager maintains a User Access List to evidence clearly user access rights, this is archived as rights are changed to evidence user access history. These access rights are reviewed at planned intervals, or as required, by the senior management.

Secure configuration process, use of utility programs, system files, or other software that might be capable of overriding system and application controls or altering system configurations must be restricted to the minimum personnel required as listed below.

Special attention is given to the control of privileged access rights. The Operations Control Centre room is locked at all times from within. Human Resources department room is locked when unoccupied.

Any visitors attending Interr HO have their ID checked upon arrival and remain with a member of the HO team at all times during their visit and will not enter areas with privileged or limited access without approval. CCTV in the HO records unlimited areas within the HO allowing monitoring of all visitors.

User Registration and Deregistration

Only authorized administrators shall be permitted to create new user IDs and access and issue any company equipment and may only do so upon receipt of a documented request from authorized parties using the approved QC forms. User provisioning requests must be submitted to the HR team and include approval from the line manager of the employee requesting additional access.

User IDs, access and equipment shall be promptly disabled or removed when users leave the organization or contract work ends. User IDs shall not be re-used and company equipment shall be returned. The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. In the case of a separation from the company, all access will be deprovisioned within the same day the offboarding request is submitted unless otherwise specified.

Information Access Restrictions

The level and type of restrictions applied by each application should be based on the individual application requirements, as identified by the data owner. The application-specific access control policy must also conform to Interr's policies regarding access controls and data management.

Prior to implementation, evaluation criteria are to be applied to application software to determine the necessary access controls and data policies.

Assessment criteria include, but are not limited to:

- Sensitivity and classification of data.

- Risk to the organization of unauthorized access or disclosure of data
- The ability to, and granularity of, control(s) on user access rights to the application and data stored within the application
- Restrictions on data outputs, including filtering sensitive information, controlling output, and restricting information access to authorized personnel
- Controls over access rights between the evaluated application and other applications and systems
- Programmatic restrictions on user access to application functions and privileged instructions
- Logging and auditing functionality for system functions and information access
- Data retention and aging features

Secure log-on controls shall be designed and selected in accordance with the sensitivity of data and the risk of unauthorized access based on the totality of the security and access control architecture.

User Responsibilities

Users shall take all measures to prevent compromise and/or theft of their access rights in accordance with the organisation's Cryptography Security Policy. They shall be expected to do this through the following:

- Maintaining authentication security, particularly regarding password and key card safety
- Securing assets assigned to them (e.g. computer and other office equipment)

If this policy is breached the Company, may take disciplinary action and may result in your dismissal without notice.

Network Access Control

Users shall have direct access only to the services and systems that they have been specifically authorised to use. Upon being granted specific authorisation, users may be allowed access to the following:

Networks – Organisations LAN/WAN
Network Services –File Services, E-mail & internet

Network and Systems access

Access to the network and systems will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. There is a formal, documented user registration and de-registration procedure for access to the network and Interr's systems.

Access rights to the network will be allocated on the requirements of the user's job, rather than on a status basis. Security privileges (i.e. 'super user' or network administrator rights) to the network will be allocated on the requirements of the user's job, rather than on a status basis. Access will not be granted until the IT Helpdesk or Super Admin registers a user by receiving the New User Request Form approved by HR.

All users to the network will have their own individual user identification and password. Users are responsible for ensuring their password is kept secret. User access rights will be immediately removed or reviewed for those users who have left the organisation.

Third Party Access Control to the Network Third party (auditors or government agencies) access to the network will only be permitted with a permission from the ISO or CEO.

Access controls apply to all networks, servers, workstations, laptops, mobile devices, cloud applications and websites, cloud storages, and services.

All customer data stored in SharePoint Online is encrypted (with one or more AES 256-bit keys) an is FIPS 140-2 Level 2 validated. Interr has the ability to control variety of devices and systems across multiple instances by using an external Remote Monitoring and Management system.

Network segregation and segmentation

Network segregation and segmentation are used by Interr to reduce our security risks in a digital environment.

Some of the key benefits of network segmentation and segregation include:

- Limiting access privileges to those who truly need it
- Protecting the network from widespread cyberattacks
- Boosting network performance by reducing the number of users in specific zones

Network Segregation

Refers to the separation of critical networks from the internet, as well as from other internal networks. It also enforces rules for communication between hosts and services.

Network Segmentation

Involves splitting larger networks into smaller segments, usually through firewalls, local area networks, and other techniques.

Protection of application service transactions

While security responsibilities will vary depending on the type of service the company uses, all staff, contractors, consultants etc will be responsible for the effective management of the data that we store and process within our business. Application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

The company will ensure that the latest software updates are used on all security assets and services – this will be completed by getting the latest systems from the approved providers of the systems the company uses. All automatic updates on all our operating systems and applications are enabled and forced to ensure all users use the latest software.

All transactional information is stored outside a publicly accessible environment (e.g. – Sage, HSBC, Nat West) and is not retained or exposed on an internet- accessible storage medium, other than those provided by the 3rd party, such as banking institutions or issued platforms, which confirm to regulated infosec standards.

Protection is incorporated and implemented in the electronic DocuSign signatures (where applicable) for any contractual or transactional details. The company uses web application firewalls among an active antivirus and a two factor authentication when logging onto any systems that handle any level 3 sensitive data – such as banking, transactional payments and any personal details. Person to person verification will be followed before any data is accessed or submitted in line with Interr's InfoSec policies and procedures.

Testing such as penetration testing and vulnerability testing will be completed on annual basis ensuring the services we use and have control over, to ensure they are secure and there are no potential weaknesses. Spot check testing on the services will be completed quarterly in line with the below protection of the log information section.

Protection of log information

Access to Interr's network, systems and communications shall be logged and monitored to identify potential misuse of systems or information, alterations, edited, deleted, overridden, etc. Logging activities shall include regular monitoring of system access to prevent attempts at unauthorized access and confirm access control systems are effective. Log servers and documents shall be kept secure and only made available to relevant personnel. These logs shall be kept as long as necessary or required for functional use, to satisfy audits and /or appropriate regulatory requirements or law. Some audit logs may be required to be archived as part of any requirements to collect and retain as evidence for a maximum of 3 years.

Interr's information systems (servers, workstations, firewalls, routers, switches, communications equipment, etc.) shall be monitored and logged to:

- Ensure use is authorized
- Manage, administer, and troubleshoot systems

- Protect against unauthorized access
- Verify security procedures and access
- Verify system and operational security
- Comply with Interr's policies and procedures
- Detect and prevent criminal or illegal activities

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit logging information to:

- Determine the activity that was performed
- Who or what performed the activity, including where or on what system the activity was performed (subject)
- Systems and objects involved
- When the activity was performed
- Alterations or deletion or edition or over riding of past events
- Status (such as success vs. failure), outcome, and/or result of the activity

The frequency of review logs shall be determined according to the sensitivity of the information stored, the function of the system, and other system requirements as determined by the Company. This is to:

- Ensure events are properly classified
- Review logging for performance delays
- Ensure compliance related logging cannot be bypassed
- Verify access to log files is properly restricted
- Assist with investigations and compliance with relevant authorities

Logs shall be protected against any security risks by permitting only the authorised personnel to have access to these logs and by completion of internal audits by independent personnel.

- Protect the information held within system audit logs in accordance with its Information Classification as stated on Interr's Information Handling policy.
- Review the activity logs of privileged users and system administrators on a quarterly basis by the Information system security managers and administrators and reviewed by the compliance team, to ensure that privileged users remain impartial and maintain accountability for the users.
- Only access, monitor, or analyse logs, network connections, or location information of individuals for legitimate business and job-related purposes.
- Keep such information confidential, and not disclose such information to others unless there is a job-related or legal requirement to do so.
- All security logs shall be backed-up and archived as required.
- Administrators shall take appropriate precautions to prevent security logging from being deactivated, modified or deleted.
- Logs, logging facilities and log configuration tools must be protected so that only authorised administrators have access and no end users may delete or alter logs. If separate log archiving facilities are used, the administrators for these facilities should be different from the administrators for the systems generating the logs in order to prevent misuse by system administrators. Access to logs must be granted on a strict need-to-know basis.
- System clocks are used to record the date and time of events in log entries, and the correct setting of clocks is important to ensure their accuracy. Inaccurate audit logs may hinder investigations and damage the credibility of log entries used as evidence.
- The confidentiality and integrity of the archived logs also need to be protected. Use only those computing resources that they have been authorised to use, and use them only in the manner and to the extent authorised.
- Do not interfere with the intended use or proper functioning of information technology resources, or gain or seek to gain unauthorised access to any resources.
- Do not circumvent or bypass security measures, requirements, or any standard protocols in place to ensure the confidentiality, integrity, and availability of Interr systems and networks.

- Asset log will only be controlled and monitored by the authorised personnel and reviewed quarterly by the compliance team to ensure accountability of all assets.

Change, Capacity and Access Management

Interr Ltd defines a change as anything that alters, modifies or transforms the operating environment of any systems, software or services that has the potential to affect the stability and reliability of in infrastructure or disrupt the business of Interr Ltd or its clients.

The change control process shall include a risk assessment, analysis of the impacts of changes and specification of security controls needed. This process shall also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained. This is in line with the SOP 23 Project Management.

Changes may be required for many reasons, including, but not limited to:

- User requests or Client's recommendations
- Changes in regulations
- Hardware and/or software upgrades or hardware or software failures
- Changes or modifications to the infrastructure
- Environmental changes (electrical, air conditioning, change of office layouts, etc)
- Unforeseen events or periodic maintenance

Each Information Technology request, including emergency requests for Change will be reviewed and prioritized by the ISO/CEO following discussion with senior management.

These changes will be monitored by the Super Admin User after receiving an approval from the CEO. All changes will undergo some level of testing depending on the complexity of the change.

During the testing process, Interr will determine that the change satisfy specified requirements, and demonstrate that it is fit for purpose and use. All testing will be completed using set up of fictitious users prior to the actual roll out of a new system or a service.

Testing may be performed by the team(s) who develop the software or by a temporary team of testers composed by selected Head Office individuals from different existing teams.

No new services, software or systems being introduced or changed will be implemented until all testing has been completed to a satisfactory level and assigned to the relevant access groups.

Security requirements – analysis and specification

Whilst Interr doesn't design our own systems or creates enhancements to our existing information systems, we use external systems as part of our service delivery and recognise the importance of protecting the security information held within these systems.

All security requirements shall be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall functional requirements for an information system as stated in the SOP23 Project Management and Change Management.

Statements of functional requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls needed to ensure the confidentiality, integrity and data availability for the information system. These specifications should consider the automated controls to be incorporated in the information system, and the need for supporting procedural controls, as listed on Interr's Data risk treatment plan and register.

All new information processing systems shall be required to be approved by the executive board of directors. Access provisioning, authorisation process and duties and responsibilities of all relevant users will be communicated and in

line with this policy as stated above and the Information handling policy. Requirements of protecting the assets and logs will be in line with the in protection of log information as stated above. Where the security functionality in a proposed product does not satisfy the specified requirement, then the risk introduced and associated controls required to address the risk should be reconsidered prior to purchasing the product. Where additional functionality is supplied which causes a security risk, this shall be disabled or the proposed control structure should be reviewed to determine if advantage can be taken of the enhanced functionality available.

Operating System Access Control and Backup

Controls shall be implemented to restrict information system access to authorised users by requiring authentication of authorised users in accordance with the defined access control policy. Controls include:

- Providing mechanisms for authentication by knowledge-, Keys &/or Keypad methods as appropriate.
- Recording successful and failed system authentication attempts
- Recording the use of special system privileges and
- Issuing alarms when access security controls are breached.

Regular and automated encrypted back-ups of all systems are in place to protect them from power failures or other disruptions caused by failures in supporting utilities.

Information Access Control

Controls shall be established and implemented to prevent unauthorised access to information held in application systems. High level clearance should only be authorised by the ISO.

Multifactor authentication

Sometimes referred to as two-factor authentication or 2FA is a security enhancement that required two pieces of evidence when logging or using a certain account. Multifactor authentication is enforced only on certain system within the company, such as company banking or payments systems.

Mobile Computing

Controls shall be established and implemented to ensure information security when using mobile computing devices. Controls shall be implemented to commensurate with the:

- Type of user(s)
- Setting(s) of mobile use and
- Sensitivity of the applications and information being access from the mobile device.

Mobile phone policy should be read in conjunction with this policy.

Policy Review and Assessment

This policy may be amended by Interr at any time in order to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.

Mick Tabori - CEO
January 2023