Demo Limited		
Access Control Policy		
ISO/IEC 27001:2013		
Issue 1	**Annex A A9.1.1** **Access Control Policy**	**Authorised By :- Directors of Demo Limited**
Page 1 of 6	**Effective Date: 25th October 2021**	**Classification :- Internal**
Issue Date: 1st April 2015	**Last Review Date: 25th October 2021**	

ACCESS CONTROL POLICY

This policy is issued to ensure that all employees, contractors and other interested parties understand and apply the business requirements for the control of access to information. It has been established, documented and is reviewed as detailed in the policy review process.

The business requires that information, information processing facilities and business processes are controlled as detailed within this policy and associated procedures. This is designed to limit access to information and information facilities. In particular network and network services controls are particularly important including users operating in public and external areas accessing sensitive or critical business applications.

Demo Company implements access controls across its networks, IT systems and services in order to provide authorised, auditable and appropriate user access. These controls are there to ensure that appropriate preservation of all data's confidentiality, integrity and availability is maintained in accordance with this policy together with Demo Company's Information Security Policy and the User Access Provisioning Process.

Access Control systems are in place to protect the interests of all users of Demo Company's computer systems (mainly servers) by providing a safe, secure and readily accessible environment in which to work and for the applicable systems to operate at optimum performance. The business requires that information, business processes and information processing facilities are effectively controlled. This policy is designed to limit the access to information and information facilities, in particular to network and network services and it includes access controls if a user is operating in a public or other external area. This policy takes into account controls specifically designed for when a user is accessing any sensitive or critical business data or application.

Asset Owner

Assets relating to access controls are under the authority of senior management who are responsible to appoint information security representatives. These representatives are therefore the appointed responsible owner of access controls and any other related security controls.

Privileged Accounts

The allocation of privileged rights (e.g. local administrator, domain administrator, root access) shall be restricted and controlled. Authorisation for the use of such accounts shall be provided upon written request and approval from a senior manager. To prevent against potential losses in the

confidentiality and/or integrity of information, access rights are only given on an individual basis and senior management should never issue privileged rights to groups or teams of people. Access rights are only given following the principles of "least privilege" and a "need to know basis". Only authorised employees documented in the Privileged Access Rights Register have privileged access to systems processing. Exceptions require written authorisation for exemption and this are to be recorded and filed. System management logs are to be updated to record suitable mandated fields and are to be monitored. System administrators are to be assigned an individual admin account for undertaking of any admin tasks and should also be given a separate standard account for performing their normal business functions.

Maintaining Data Security Levels and Classification

Every user should understand the sensitivity of data and treat it accordingly. The Privileged Access Rights Register and the User Registration and De-Registration Process sets the standards for users access rights. Access permissions to information is primarily based on the sensitivity of the information and its classification level as established by 's Asset Classification Procedure.

Information security levels and class applicable rules applicable to information labelling, need to take into account classification as well as the relevant handling of various types of assets. This is done in accordance with Demo Company's Asset Classification Procedure. All information is to be rated with an appropriate classification and should include a defined handling requirement for the information's classification. Classification of media should be visually identifiable. All data needs to be handled appropriately as well as stored suitably and always maintain its level of classification.

Review and Monitoring

This policy needs to be periodically reviewed and updated as detailed in the Information Security Policy Review Process. The review of access controls is outlined in the User Access Rights Review Process. The review shall be documented and senior management shall sign off the review to enable the continuation of authority detailing all users' access rights. An adequate set of technical control implementations or processes are in place for the monitoring of access. Access is managed and controlled through a system of access controls, identification & authentication methods, as well as via audit trails.

Access Control Rules

Access control rules are enhanced by a formal procedure which includes a description of the defined responsibilities of personnel. Segregation of access control roles are applied wherever possible. Access to confidential, restricted and protected information is limited to authorised persons only

whose job responsibilities require it. This is determined by the data owner and is stipulated in accordance with Demo Company's User Access Provisioning Process.

Access rights are given following the principles of "least privilege" and a "need to know basis". Access to everything is in general forbidden, unless expressly permitted and in writing. Requests for access permission to be granted changed or revoked is to be made in writing and in line with the Removal or Adjustment of Access Rights Procedure.

A password control procedure is in place to ensure appropriate passwords which are alpha-numeric and not guessable are in place according to Demo Company's Password Control Procedure. This procedure ensures that password issuing, strength requirements, changing and control is managed through a formal process.

Information security awareness, education and training, and use of secret authentication information is communicated to all employees. All users are to be informed about their expectations, expected knowledge, and skills related to information security and other related information security policies.

Access Rights

Consistency between access rights and information classification policies should always be in place, especially with regards to systems and networks.

Removal of Access Rights

The User Registration and De-registration Process describes the process if an employee's role or status changes and further describes the process and procedure that needs to be implemented to ensure that a user's information system access is properly updated to reflect the new role. System users that may need additional access to bypass security mechanisms, for any reasons, needs to be first given formal authorisation by senior management.

Logical Access and Physical Access Restrictions

Two principles to be implemented are:

1. The need to identify i.e. which granted access should be given to perform applicable tasks.
2. The need to use i.e. which access permissions are applicable for a user to perform his task efficiently and effectively, while keeping information security at a suitable risk level.

Legislation and Contractual Obligations

Relevant legislation and contractual obligations, regarding limitation of access to data & services should be taken into account when setting access controls as well as when establishing Demo Company's Information Security Policy, Risk assessment and Treatment Plan and User Access Provisioning Process.

Senior management are to ensure that information security responsibilities are included in an employee's job responsibilities and employment contact. Privacy and protection of personally identifiable information should always be followed by the company and its employees. All personal information that should be retained as per relevant legislation is adhered to by the organisation and its staff.

Compliance includes being audited by an appropriate body and is carried out at least once every year. Information Security Policy Review Process is completed annually to help ensure that appropriate policies are in place and that the scope includes all information assets, people, processes and legislation.

All relevant legislation for cryptographic controls is complied with.

Network and Network Services

Limiting the access to information and information facilities is vital to ensure Demo Company's information security. In particular network and network services controls are of particular importance and are further described in Demo Company's Network Security Procedure.

The following is taken into consideration for network and network services access controls:

- Authorisation procedures to determine who is allowed to access to which networks/services;
- Management controls and procedures to protect access to network connections/services;
- The means used to access networks and network services;
- User authentication requirements for accessing various network services; and,
- The monitoring of the use of network services.

Networks connected to multifunction devices may be capable of transmitting confidential information and should therefore have similar controls to normal computers i.e. they need to include access controls and content management security etc. All application services on public networks needs to be appropriately secured. Details of internal network and system configuration or other sensitive technology information should not be publicly disclosed or available to unauthorised personnel. Information access should always be kept restricted and all removing and disabling of default accounts needs to be strictly adhered to.

Significant Events

Archiving of records for all significant events should be recorded and retained. Logs are to be retained for a period decided by senior management depending on the logs relevancy.

Information Asset

System users are responsible for the information assets provided to them and to carry out their official responsibilities. They need to handle all information assets with due care and operate them in line with Demo Company's policies and procedures.

Equipment Siting and Protection

Equipment is located in protected areas with access controls to minimise risk of theft and/or espionage. Information processing facilities and the managing of sensitive data is positioned carefully to reduce the risk of any information being viewed by unauthorised individuals. Storage facilities should are secured to avoid unauthorised access and password protection and monitoring should is used to reduce this risk. The information security policy relating to this is the Equipment Siting and Protection Procedure.

Secure Disposal and Re–Use of Equipment

Demo Company's equipment is assigned an owner and is to be protected in a manner corresponding with its value to the organisation and/or its customers. In order to preserve the confidentiality of Demo Company's information assets, senior management should ensure that information is protected against unauthorised access throughout its lifecycle, and this includes the lifecycle of the hardware where the information may reside. Sensitive information should not be left on storage media or other equipment (e.g. hard drives) in the event that the equipment is decommissioned or repurposed. This is procedure is further described within Secure Disposal of Media Procedure.

Unattended User Equipment

Access to a system is suspended after specified number of logon attempts. When a staff member no longer needs access to a system as a result of the employees changed role, access is removed from that system for that specific staff member. All accounts that are inactive for more than 3 months are suspended. These procedures are further described in Demo Company's Removal or Adjustment of Access Rights Procedure, Equipment Siting and Protection Procedure and Password Control Procedure.

Access control to program source code

The organisation restricts access to source code to authorised personnel and logs monitor access and change control is managed as defined in the separation of environments procedure.

Responsibilities and Procedures

Management responsibilities in terms of termination or change of employment should have a clear set of responsibilities and procedures which is more detailed in Demo Company's Termination or Change of Employment Controls for Employees and Contractors and Removal or Adjustment of Access Rights Procedure.

Demo Company has a defined set of operational information security responsibilities for information security management and further ensures that all employees are familiar with its Information Security Policies.

Information security policy for supplier relationships also has a process and procedure which is detailed in Demo Company's Supplier Relationships Policy, Supplier Agreement Process and Service Management Relationship Process.