Access Control Policy

Reference: GDPR DOC 2.3
DocumentKits Issue No: 1.0
DocumentKits Issue Date: 25/02/2022

1. Scope

This policy applies to Organisation Name's information systems and mechanisms used to connect to or access those systems.

2. Definitions

Access control is the process by which a User is granted access to information and systems necessary to perform their roles. It incorporates information classification and User authentication.

Information classification is the system of labelling information to set out how that information can be used, and by whom/by which applications.

<<Content removed for sample purposes>>

3. Policy

Organisation Name controls access to information on the basis of business and security requirements.

Access control rules and rights for each
"User/group of users"

are clearly stated in standard User profiles. These rules and rights address the User's needs for access to specific information and systems.

The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.

The access rights take into account:

- Premises access control – unauthorised persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems are located.

SAMPLE

- System access control – unauthorised access to data processing systems is prevented.
- Data access control – persons entitled to use a data processing system gain access only to the data to which they have a right of access.
- The need to prevent personal data from being read, copied, modified or removed without authorisation.
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- <<Content removed for sample purposes>>
- Access that requires specific permission before enactment.
- Any privileges that Users need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

Organisation Name has standard User access profiles for common roles "(see Access Control and User Administration Procedure)."ACCEPT TEXT

Management of access rights across the network(s) is facilitated by "Active Directory."ACCEPT TEXT

User access requests, authorisation and administration are segregated as described in the "Access Control and User Administration Procedure."ACCEPT TEXT

User access requests are subject to formal authorisation, periodic review and removal.

Users' identities are verified through formal authentication, the level of which is a factor of access control. Rules for authentication are set out in the "Access Control and User Administration Procedure."ACCEPT TEXT

Document owner and approval

SAMPLE

The Information Security Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.

The current version of this document is available to
"Specify which members of staff this document is intended for"

and is published
"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the Master List of Document Approval.

This document contains material that is distributed under licence from IT Governance Publishing Ltd. © IT Governance Publishing Ltd.

SAMPLE