Access Control Policy

Reference: GDPR-C DOC 9.1.1
DocumentKits Issue No: 1.0
Organisation Issue No:
DocumentKits Issue Date: 15/11/2019
Organisation Issue Date:

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

2. Access control rules and rights to applications, expressed in standard user profiles, for each user / group of users are clearly stated, together with the business requirements met by the controls.

3. 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.

4. The access rights to each application 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.
- System access control – access to data processing systems is prevented from being used without authorisation.
- 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.
- Personal data cannot be read, copied, modified or removed without authorisation.
- The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the system(s) and network(s)
- Data protection (EU GDPR) and privacy legislation and contractual commitments regarding access to data or services.
- The 'need to know' principle (i.e. access is granted at the minimum level necessary for the role).
- 'Everything is generally forbidden unless expressly permitted'.
- Rules that must always be enforced and those that are only guidelines

"which rules and how do you take this into account?"

• Prohibit user initiated changes to information classification labels (see Information Classification Procedure).
"how do you do this?"

• Prohibit user initiated changes to user permissions.
"how do you do this?"

• Enforcing rules that require specific permission before enactment.
"how do you do this?"

• Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

5. Organisation Name has standard user access profiles for common roles in Organisation Name (see Access Controls Rules and Rights Procedure).

6. Management of access rights across the network(s) is
"done how?"

7. User access requests, authorisation and administration are segregated as described in Access Controls Rules and Rights Procedure.

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

Document Owner and Approval

The Information Security Manager is the owner of this document and is responsible for keeping it up to date.

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 Master List of Document Approval.