Access Control Policy

Reference: NIS DOC B2-01
DocumentKits Issue No: 1.0
DocumentKits Issue Date: 25/08/2021

1. Organisation Name controls access to information and systems on the basis of business and security requirements as determined by the Information Security Policy.

2. Access control rules and rights to applications and networks, expressed in standard User profiles, for each
"User/group or Users"

are clearly stated, together with the business requirements met by the controls, in Access Controls Rules and Rights.

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

4.
"By default, the organisation prohibits remote access to network and information systems in accordance with the Network Access Control Policy."

5. The access rights to each application take into account:

a) 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
"systems and network(s)."

b) Data protection (
"Data Protection Act 2018, EU General Data Protection Regulation, privacy and information security (NIS Directive/Regulations)"

),
"and other legislation and contractual commitments"

regarding access to data or services.

c) The 'need to know' principle (i.e. access is granted at the minimum level necessary

SAMPLE

for the role).
d) 'Everything is generally forbidden unless expressly permitted'.

e) Rules that must always be enforced and those that are only guidelines.
"Which ones? How do you take this into account?"

<<f-l removed for sample purposes>>

6. Organisation Name has standard User access profiles for common roles in Organisation Name (see Access Control Rules and Rights).

7. Management of access rights across the network(s) is
"Detail how this is carried out."

This is done in line with User Access Management.

"8. If personally identifiable information (PII) processing is provided as a service (whether through a Cloud service or some other mechanism), describe how customers' user access rights are managed and controlled, including termination. Refer to another document if necessary.

9. Where Organisation Name uses Cloud services, it will ensure that access to information in the Cloud services can be restricted in accordance with this policy, including restriction of access to Cloud services, Cloud service functions, and data stored in the Cloud service, and ensure that such restrictions are realised."

"10."ACCEPT TEXT

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

"11."ACCEPT TEXT

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

"12."ACCEPT TEXT

"All/privileged"

User access is logged and monitored in line with the Information Security Monitoring Procedure.

Document owner and approval

The Information Security Manager is the owner of this document and is responsible

SAMPLE

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.

SAMPLE