ACCESS CONTROL POLICY (TIER 1)

Document Control
Reference: GDPR-C DOC 9.1.1
Issue No:
Issue Date:
Page: 1 of 2

1 Cognus 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:

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

b. System access control – access to data processing systems is prevented from being used without authorisation.

c. 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.

d. Personal data cannot be read, copied, modified or removed without authorisation.

e. 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 network(s).

f. Data protection (EU GDPR) and privacy legislation and contractual commitments regarding access to data or services.

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

h. 'Everything is generally forbidden unless expressly permitted'.

i. Policies and procedures that must always be enforced and those that are only guidelines.

j. Prohibit through sharing knowledge and understanding of the importance of accurate data classification any user initiated changes to information classification labels (see GDPR-C DOC 8.2).

k. Prohibit through robust control policies and procedures user initiated changes to user permissions.

l. Enforcing through clear policies and appropriate action to ensure rules require specific permission before enactment.

m. 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 Cognus has standard user access profiles for common roles in Cognus (see GDPR-C DOC 9.1.2).

6 Management of access rights across the network(s) is by the London Borough of Sutton. Access is restricted to the level required to undertake individual jobs roles. This is managed through New Starter Forms for new employees and through the LAN Desk Hub. In both cases approval is sought from managers within the business prior to access to systems and data being granted.

7 User access requests, authorisation and administration are segregated as described in GDPR-C DOC 9.1.2.

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

Document Owner and Approval

The Head of Resources is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff on the Intranet and is published.

This policy was approved by the Managing Director on 22/05/2018 and is issued on a version controlled basis under the signature of the Managing Director.

Signature: R.A. Burley Date: 25/05/2018

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Managing Director	25/05/2018