INFORMATION SECURITY CLASSIFICATION GUIDELINES (TIER 2)

1. Scope [ISO 27002 Clause 8.2.1]

All Cognus's information assets and services, and personal data activities are classified, taking into account their legality, value, sensitivity and criticality to Cognus.

2. Responsibilities

2.1 The owner of each asset is responsible for its classification, for ensuring it is correctly labelled and for its correct handling in line with its classification.
2.2 The intended recipient of any information assets sent from outside Cognus becomes the owner of that asset.
2.3 The Head of Resources is responsible for maintaining the inventory of assets and services together with their classification levels.
2.4 The Head of Resources is responsible for the technical labelling mechanisms.
2.5 The Head of Resources is responsible for the creation, maintenance and review of electronic distribution lists and for ensuring that they conform to this security classification system.
2.6 All users of organisational information assets (including mobile phones, PDAs and other peripherals) have specific responsibilities identified in their user agreements.
2.7 Managers / owner are responsible for ensuring that data sent by mail, voicemail, voice etc and sensitive documents (including cheques, invoices, headed notepaper) are handled in line with the requirements of the GDPR.

3. Classification

3.1 Cognus classifies information into four levels of classification: confidential, restricted, private and public.
3.2 The classification level of all assets is identified, both on the asset and in the information asset inventory.
3.3 The classification information must be included in the document footer, which must be manually set to appear on all pages of the document, or on the media on which it is recorded, in line with Clause 8, below.
3.4 Information received from outside Cognus is reclassified by its recipient (who becomes its owner) so that, within Cognus, it complies with this procedure.
3.5 Information that is not marked with a classification level is returned to its sender for classification; if it cannot be returned, it is destroyed.
3.6 The classifications of information assets are reviewed every 12 months by their owner and if the classification level can be reduced, it will be. The asset owner is responsible for declassifying information.
3.7 Confidential: this classification applies to information that is specifically restricted to the Board of Directors and specific professional advisers.

3.7.1 Information that falls into this category must be marked 'Confidential', and its circulation is kept to a minimum with the names of the people to whom it is limited identified on the document.

3.7.2 Examples of confidential information might include information about potential acquisitions or corporate strategy, or about key organisational personnel, such as the Managing Director.

3.7.3 Confidential information sent by email must be encrypted (if sent to anyone outside of Cognus Limited) and digitally signed and sent only to the e-mail box of the identified recipient.

3.7.4 Confidential information can only be sent by fax if the nominated recipient is available to receive it directly from the fax machine.

3.7.5 Confidential information can only be processed or stored on facilities that have been assessed as providing adequate security for such information. This classification is recorded on the information asset inventory and/or data inventory (DPIA Tool GDPR REC 4.4).

3.7.6 The amount of information that falls into this category should be carefully limited; the cost and operational inconvenience of protecting it properly is such that it needs only to be information whose release can significantly damage Cognus.

3.8 Restricted: information of this category is restricted to Employees/Staff above the level of:

3.8.1 Examples of restricted information include records relating to draft statutory accounts, which might be available to everyone in senior management, or implementation plans for corporate restructuring, which senior managers need to work through prior to their being rolled out.

3.8.2 Information related to children and young people will always be classified as restricted information which may be available only to colleagues involved in supporting the child or young person or to those involved in the management of the service being provided.

3.8.3 Restricted information sent by email must be encrypted (unless sent to another Cognus email address) and digitally signed and sent only to the e-mail box of individuals known to be allowed to receive such information.

3.8.4 Restricted information sent by mail must be sent using Special Delivery tracked mail.

3.8.5 Restricted information can only be sent by fax if a recipient from the required level is available to receive it directly from the fax machine.

3.8.6 Restricted information can only be processed or stored on facilities which have been assessed as providing adequate security for such information. This classification is recorded on the information asset inventory and/or data inventory.

3.9 Private: this classification covers all information assets that have value but which do not need to fall within either of the other categories.

3.9.1 Everyone employed by Cognus is entitled to access information with this classification.

3.9.2 This information has no restrictions in terms of how it is communicated, other than that it is not cleared for release outside Cognus.

3.10 Public: this is information which can be released outside Cognus.

4. Labelling [ISO 27002 Clause 8.2.2]

4.1 Documents are labelled as set out above, in the document footer. Documents that do not have footers are marked by addition of a physical, stick-on label.
4.2 Removable and storage media (CD-ROMs, USB sticks, tapes, etc.) are labelled according the Information Security Classification Guidelines.
4.3 Electronic documents and information assets are labelled by the author.
4.4 All emails have a standard disclaimer available from the Business Support team to the effect that the views expressed in the e-mail are those of the sender alone and do not reflect the views of Cognus.

5. Handling [ISO 27002 Clause 8.2.3]

5.1 Information assets can only be handled by individuals that have appropriate authorisations.
5.2 The requirements for transmission, receipt, storage and declassification of classified and restricted information are described above. Destruction of information media can only be carried out by someone who has an appropriate level of authorisation.
5.3 Cognus requires that confidential documents are only circulated to those included as the intended audience.
5.4 Portable and storage media (including spooled media) must be moved, received and stored on the basis of the highest classification item recorded on them, and are subject to the same physical security controls as the highest classification.
5.5 For agreements with external organisations (GDPR-C DOC 15.2.2) which include information sharing, include a matrix for translating their security classifications into this one.

Document Owner and Approval

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

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

This procedure was approved by the Head of Resources and the Head of Resources / Head of Resources on 19 May 2018 and is issued on a version controlled basis under his signature.

Signature:  Date:19/05/2018

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Head of Resources	19/05/2018