Catena
Inspection & Engineering Services Ltd
Lifting Solutions & Supplies

CHR027 Document Security Policy

JULY 2025 | ISSUE 2

Confidential and Sensitive Information / Documents

As part of your duties, you may receive confidential information of a sensitive nature (which include particularly commercially sensitive information), whether as a hardcopy document, electronic, verbal or any other means. It is expressly not permitted to divulge this information to anyone outside of the company. In certain cases it may not be permitted to share with other people within the company, but this will be identified at the time you might receive such information.

Official Sensitive Classification Documents

Our customers may occasionally issue to us hardcopy documents or electronic data (such as CD's, USB's, via Egress) which are classified as 'Official Sensitive' or above. In this case we may need to limit who these are accessed by, subject to relevant security clearance (minimum BPSS – the IMS Manager holds the register of BPSS Cleared Personnel, please ask if you are unsure). If you are authorised to handle these levels of documents, you MUST ensure the security of them at all times. They must not be issued to a supplier by email, only by post / hand delivery, and with an accompanying SAL Flow Down Letter. They must not be issue to the workshop regardless of security clearance as this is an uncontrolled area. In the office they MUST be locked away (in locked drawers with the key removed) when not being used.

When on a desk, do not leave then unattended, and be aware at all times of who is in the office, particularly non-Catena personnel.

When dealing with electronic data, if copies of this are required, this may be done by accessing the data on your PC and downloading only to your local desktop. A new electric version can be created using the same password protocols as the original. After this, the file MUST be permanently deleted, and never4 stored on the central company server.

All Other Documents

Any other documents within the office and workshop, should be stored in such a way that sensitive data is not available to other employees (where applicable) and in particular to non-Catena personnel.

Examples

Examples of documents may include but are not limited to: Invoices, Accident Records, NCR's, HR Records.

Examples of Non-Catena Personnel may include but are not limited to: Service Providers (NDT, Painters, Machinists), Maintenance Sub Contractors (Builders, Electricians, Plumbers), Cleaning Company, Pest Control Company, Customer Visitors, Supplier Visitors, Delivery Drivers & Hauliers

Incident Management

Incidents shall be reported to the Managing Director or the IMS Manager and then the below action shall be taken.

- Detect how and where any breach has occurred.
- Define the resolution
- Plan for the recovery once the above has been completed

Roles and Responsibilities

Breaches or suspected breaches shall be reported to the Managing Director or the IMS Manager

Any personnel found to have violated this security policy shall be subject to Disciplinary Action for Gross Misconduct and the Policy for this shall apply.

BPSS Cleared Personnel shall ensure they understand their responsibility for control of security of the document or electronic data

Any queries on this shall be directed to the IMS Manager