7. MANAGEMENT OF SPECIAL ACCOUNTS

Emergency Account

In order to ensure that, even in emergency situations, the use of all the functions of the company's IT systems and access to company data areas is permitted (unexpected absence of users, loss of password, etc.), the System Administrators are allowed to delete and reset user passwords.

Administrators will do so at the request of the relevant manager in charge or a member of the company management, or at the request of the person concerned.

This request must be "formalised" by sending an authorisation email to the Service Desk (support@cembre.com)

The password 'reset' operation is in any case tracked in the IT system and the new access is identified by the newly generated password, thus protecting the user from misuse of his/her password.

Collective accounts

In some particular cases, it is necessary to create accounts that do not relate to a single individual, but to several users at the same time.

This need arises from the convenience/need for several users to share a single resource (e.g. a PC).

Of course, if the possibility of tracking operations on the systems is lost or impaired, this option is only allowed in cases where the functional profile of the users provides limited functionality and is in no way detrimental to the security and business damage that could result from incorrect or malicious use of the account.

In cases where this is possible, it is the responsibility of the Line Manager or a member of his/her staff to make the request by sending an e-mail to the Service Desk (support@cembre.com), stating the reasons for the request and classifying the user groups to be enabled (e.g. "Warehouse personnel", or "MCN operators" etc.).

The change request must be validated through the authorisation workflow prepared in Jira by the Line Manager if he/she is not the requesting party.

External Personnel/Consultants' Accounts

There are also accounts that can be created for external staff working as auditors, consultants or specialists in specific areas or projects.

Here too, the Line Manager or a member of the manager's staff in the area in which the external personnel are to operate must send a request via the Service Desk (support@cembre.com) asking for the necessary accounts to be created, specifying the areas and expected duration.

Administrators' Accounts

The System Administrator's User and Password are kept in the safe in the Personnel Office, the key to which is kept by the Data Protection Officer.

8. DEACTIVATING UNUSED ACCOUNTS AND SAFEGUARDING STORED DATA

Unused Accounts

Login credentials not used for more than six months are deactivated.

With regard to the authentication systems for access to the IT systems, periodic checks will be carried out by the IT-STE Manager and his staff in order to keep the system free of active and unused credentials for a period longer than six months.

Deletion of Corporate and Personal Data

In order to prevent data of company interest or possibly personal information from being made available to third parties and in any case to unauthorised personnel, particular care must be taken in the following cases:

- Decommissioning (scrapping) a computer and its storage units
- Reassigning a computer to another user.

In the first case, the storage units are removed from the computer and rendered mechanically unusable.

In the second case, the units are formatted at a low level using an appropriate tool which, through repeated and specific deletion cycles, completely erases the information content.

ANNEX f)

LIST OF SYSTEM ADMINISTRATORS

Resource name
BERTINI ROBERTO
BELLANDI ALESSANDRA
PERSIANI ERMES
DOLDI FRANCESCO
BROCCHETTA ANDREA
TURATI ANDREA
PINTOSSI PAOLO
PARISI ANGELO ANDREA
LIBERO STEFANO
GUERINI DIEGO CARLO
CROPELLI RENATO