PLANET SECURITY

CYBER | ENERGY | WATER

Security Procedure

PRO.AC.L1-3.1.1

Organizational Security Procedure

POL.AC.L1-3.1.1 (Recap)

All CLIENT information systems that store, process, or transmit CUI shall employ Role Based Access Control (RBAC) to limit system access to only authorized users of CUI. Furthermore, all processes shall be visible and identifiable to both system administrators and the client user who is logged in (client user respective processes only). All devices which have the capacity to view CUI shall be identified, contractually covered by Planet Security, Inc. The use of shared accounts and/or passwords is prohibited.

Executive Procedure:

Executive management shall prepare and maintain a list of Authorized Users who are allowed to access (READ) CUI. This list shall be updated in REAL TIME as Authorized Users are transferred in, out. Revocation of access to CUI shall be performed BEFORE actions such as terminations and transfers.

Administrative Procedure:

System Administrators shall utilize Microsoft AGDLP to implement RBAC within the organization for all devices that store, process, or transmit CUI.

Soft-Copy End-User Procedure:

Users of soft-copy CUI shall access it from a covered workstation within the CPE environment only.

CUI shall not be stored saved locally on any workstation or device that has not been sanctioned for the persistent storage of CUI.

If Modifying or Creating CUI, Save back to the appropriate location on the CPE Server- do not save local copies for any reason.

Hard-Copy Operational Procedure:

A Locking File Cabinet has been installed in or around the shop floor.

Hard-copy CUI shall reside within the File Cabinet at all times when not in direct use by an Authorized Person.

Morning Procedure - Unlocking the CUI File Cabinet:

1. Unlocking shall require two persons to be present.

2. Verify that the file cabinet is locked upon arrival. Second Person will verify that it is locked.
3. Once Unlocked, the CUI Log shall be verified to be in the very front of the top drawer.

Daily Procedure - Check-out/Check-in:

1. Authorized Users of CUI shall "Check-out" only the necessary CUI assets to perform the business at hand.
2. Only one CUI asset (Traveler, Document, etc.) may be checked out at a time and must be returned when no longer needed (Job complete, end of shift, other).

Evening Procedure - Verifying all CUI is Accounted For the CUI File Cabinet, Locking the CUI Cabinet:

1. Reconciliation and Locking shall require two persons to be present.
2. Verify that all SHEETS are accounted for. Count them individually by sheet number.
3. Once the CUI Log is reconciled, Place the log binder in the very front of the top drawer.
4. Lock the CUI File Cabinet. Second Person will verify that it is locked.

Structure of CUI Log:

1. Each sheet within the CUI Asset is tracked independently (Document one may contain sheets 41-56- when checking in or out, verify EACH sheet is present)
2. When new CUI is printed, use sequential numbering PER SHEET (Not per document- there is a field on the log for which sheets are contained within each document)
3. When a sheet is ruined, destroyed, or otherwise no longer functional- it must be shredded using the CUI SHREDDER that was provided under Contract. Only this shredder may be used for this purpose. Once destroyed, log the disposition of the SHEET(s) in the log in appropriage column and sign your name as an attestation that you did the work appropriately.
4. If replacement sheets are printed to continue the business, make sure to sequentially mark the sheet, and include it within the CUI Asset. Ensure that you update tehe sheets column of the document to include the new sheet number. The old sheet number will no longer be tracked here as it was noted as destroyed in its own row in the log.

This policy Last Updated on 9 May, 2025