Physical Security

Policy PS0001/PS0001.02

Recommendations:

1. Type of physical access to the facilities itself is not mentioned so I recommend standardizing physical entry into the facility.
2. Install a key card reader at entrances to check who enters the building and ensure that no one unauthorized enters the building.
3. If employees are not trained on the dangers of tailgating, design a program to inform them. (Tailgating is when you follow behind someone who has authorized access into the area without scanning your own card).
4. There are no mentions of video recording devices being in use in these facilities. If there are not security cameras installed, I would recommend installing cameras at all entry and exit points for the building and cameras outside high security rooms, and wherever else deemed necessary.
5. No mentions of standards of security of a door, will there be sensors installed to ensure that the door is actually closed when it should be?
6. For extra secure areas, use man traps to ensure tailgating does not happen.

Policy PS0002/PS0002.02/PS0002.04

1. There is nothing written about how often the list of authorized users is audited. Depending on how well the systems are hooked up into computer systems, there is potential that users who were given access to server rooms for a period of time and have not been removed and this should be checked about once a month or more often to see if people who shouldn't be on the authorized list should be taken off the list.
2. Access logs are not reviewed often enough, it's stated that it should be reviewed at least monthly, however I would recommend a hard-set interval of once a week for sensitive information.
3. This does cost money…however…I recommend that all entry and exit points be keycard access only with a key backup and if a key backup IS used, the appropriate people should be alerted that entry was gained into a room without automated electronic record of the event occurring.
4. Doors should not have any sort of window that allows visibility into the room. If possible, apply a solid or opaque film over glass to disallow peering into the room.
5. Only Restrictive/Sensitive server rooms have multi-factor access control, while operational server rooms only require to be locked. Operational doors should also have at least keycard access (more than just a key because keys can be duplicated easily).