**Protect**

* In here, basically it implements the appropriate safeguards to preserve the availability of the critical infrastructure services.
* This particular core function consists with multiple sub-categories as following.

1. Access Control
2. Awareness & Training
3. Data Security
4. Information Protection Processes & Procedures
5. Maintenance
6. Protective Technology

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Access Control** | **Manage identities and credentials for authorized devices and users.** |  |  |  |  |
| **Manage and protect physical access to assets.** |  |  |  |  |
| **Manage remote access.** |  |  |  |  |
| **Manage access permissions.**  **Ex :-** *least privileges* |  |  |  |  |
| **Protect network integrity and utilize appropriate network segregation.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Awareness & Training** | **All users are informed and trained.** |  |  |  |  |
| **All privileged users understand their roles and responsibilities.** |  |  |  |  |
| **All 3rd party stakeholders understand their roles and responsibilities.** |  |  |  |  |
| **Senior executives understand their roles and responsibilities.** |  |  |  |  |
| **Physical and information security personnel understand their roles and responsibilities.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Data Security** | **Protect data-at-rest.** |  |  |  |  |
| **Protect data-in-transit.** |  |  |  |  |
| **Formally manage assets during removal, transfer and disposition.** |  |  |  |  |
| **Ensure adequate capacity to maintain data availability.** |  |  |  |  |
| **Protect against data leaks.** |  |  |  |  |
| **Verify software, firmware and information integrity.** |  |  |  |  |
| **Maintain separation between the development and testing environment and the production environment.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Information Protection Processes & Procedures** | **Create and maintain baseline configuration of information technology and systems that control production and distribution.** |  |  |  |  |
| **Manage systems through a System Development Life Cycle.** |  |  |  |  |
| **Control system configuration changes.** |  |  |  |  |
| **Maintain and test information backup procedures.** |  |  |  |  |
| **Adhere to policies and regulations for the physical operating environment for organizational assets.** |  |  |  |  |
| **Destroy data in accordance with policy.** |  |  |  |  |
| **Continuously improve protection processes.** |  |  |  |  |
| **Appropriately share the effectiveness of technology used for protection of systems and assets.** |  |  |  |  |
| **Manage response and recovery plans.** |  |  |  |  |
| **Test response and recovery plans.** |  |  |  |  |
| **Include cybersecurity in human resources practices.** |  |  |  |  |
| **Develop and implement a vulnerability management plan.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Maintenance** | **Use approved and controlled tools to timely perform, repair and log maintenance and repairs.** |  |  |  |  |
| **Approve, log, and perform all remote maintenance of organizational assets to prevent unauthorized access.** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sub Function** | **Description** | **Readiness** | | | |
| **Informal** | **Under Development** | **Already Established** | **Not Defined** |
| **Protective Technology** | **Create, document, implement, and review audit / log records.** |  |  |  |  |
| **Protect and restrict use of removable media.** |  |  |  |  |
| **Limit access systems & assets to the minimal level necessary to maintain normal functioning.** |  |  |  |  |
| **Protect communications and control networks.** |  |  |  |  |