

INFORMATION SECURITY

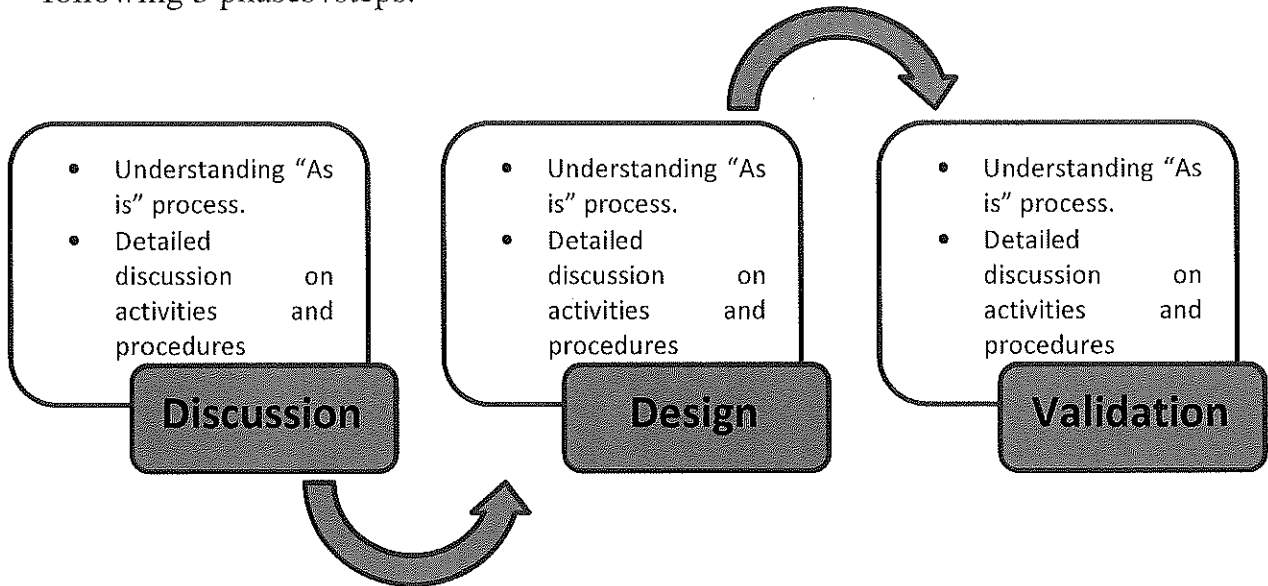
STANDARD OPERATING PROCEDURES



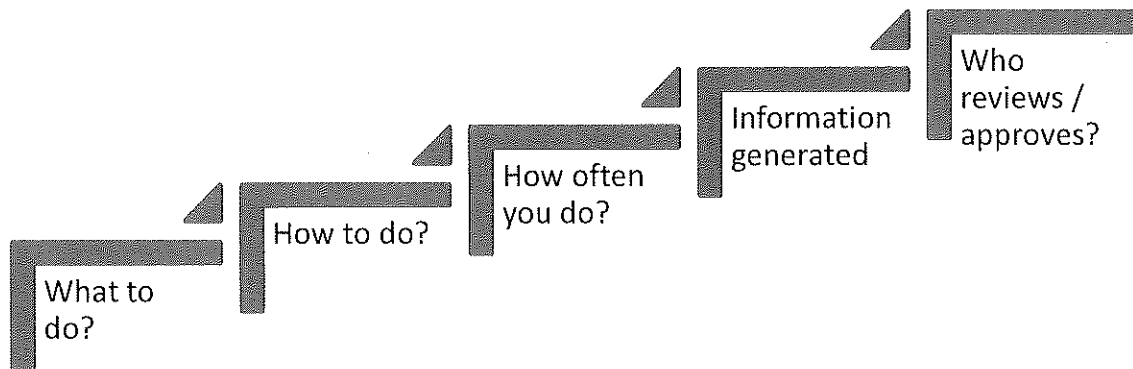
AGI Greenpac Limited

Procedure Followed

Documentation of this Standard Operation Procedures was carried out in the following 3 phases /steps.





Having well documented and structured Standard Operating Procedures (SOPs) is the best way to streamline the business processes. SOP's not only lists all tasks that are important for organizational growth but also prescribed the responsibility and procedures to perform those tasks. The following has been addressed through this SOP.



SOP Number: DS01

Information Security

| Version 2.0 | | | |
|-------------|---------------------|------------------------------|---|
| | Name | Sign Off Date | Sign |
| Reviewed By | Mr. Prashant Kunjir | 25 th April, 2024 |  |
| Approved By | Mr. Anjaiah Surgi | 25 th April, 2024 |  |
| Reason | SOP Revision | Implementation Date | 25 th April, 2024 |

| Modified By | Reviewed By | Approved By | Version No. | Reason for Change | Implementation Date |
|-------------|-------------|-------------|-------------|-------------------|------------------------------|
| | | | 2.0 | Process Change | 25 th April, 2024 |

| | |
|------------------|----------------------|
| SOP Number: DS01 | Information Security |
|------------------|----------------------|

TABLE OF CONTENTS

- | | |
|---------------------------|---|
| 1. Objective: | 5 |
| 2. Access Control Policy: | 5 |

1. Objective:

- I. Information security procedures are designed to ensure all end users and networks within an organization meet minimum IT security and data protection security requirements.
- II. This procedure is applicable to all data, programs, systems, facilities, infrastructure, authorised users, and third-party users.
- III. Information Security procedure ensures the confidentiality, integrity, and availability of the information.
- IV. Information security procedures provide protection to the entire organization and enhances company work culture.
- V. Information Security procedure provides defence against cyber-attacks.

2. Access Control Policy:

- I. Access control policy outlines the security controls, who is responsible for security controls, access controls, network security.

a) Physical Access Control Policy:

- I. Physical access to the information resources is to be controlled with strong identification and authentication techniques.
- II. Access Cards should be used for physical access.
- III. Access Cards must not be reallocated to another individual bypassing the return process.
- IV. In case of loss of access cards, the same should be informed to the IT and Admin Facility.
- V. Security officer must remove card/key access rights of individuals that change role (in Company) or separated from their relationship with (company)
- VI. Staff with authorization to enter such areas should be trained with information on the potential security risks involved.

b) Logical Access Control Policy:

I. Managing User Access and Password:

- Access control list should be maintained with the list of access and their privileges or access rights.
- All users, contractors, and vendors having access to SOMANY IMPRESA systems are responsible for taking appropriate steps to select and secure their passwords.
- For detailed information regarding User Access and Password management refer *User Management and Authorisation* policy.

II. Securing unattended workstations:

- User will be responsible for safeguarding the information assets installed.
- Users will protect the personal computers and terminals with adequate controls (Workstation locks, passwords) when not in use

and will close all application sessions, log off and shutdown the computer/ monitor when leaving for the day.

III. Controlling access to operating system:

- Access to operating system commands is restricted to those persons who are authorized to perform systems administration.
- Access to operating system is restricted by implementing security measures, keeping the programs up to date with latest versions and patching for Windows operating systems to protect the sensitive computing system.
- Security measure as firewalls, endpoint protection systems are in place. Firewall configuration should be set to allow only traffic from known, approved IP addresses and ports.

IV. Monitoring System Access and Use

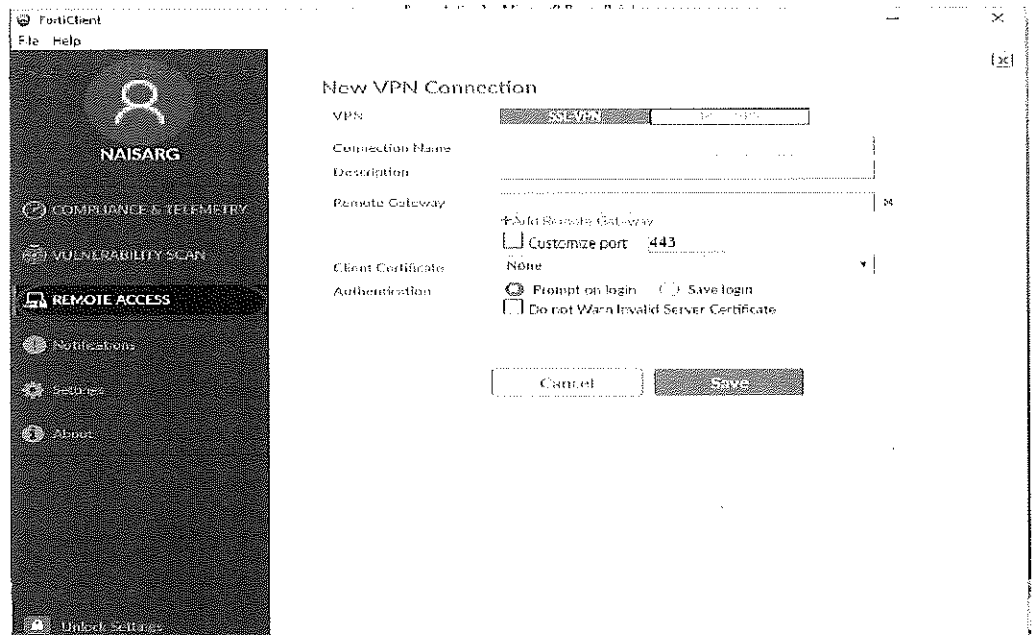
- Unused and unnecessary computer programs should be evaluated and deleted/cleaned from systems in regular intervals through Endpoint protection systems.

V. User End-Point Device Protection Policy

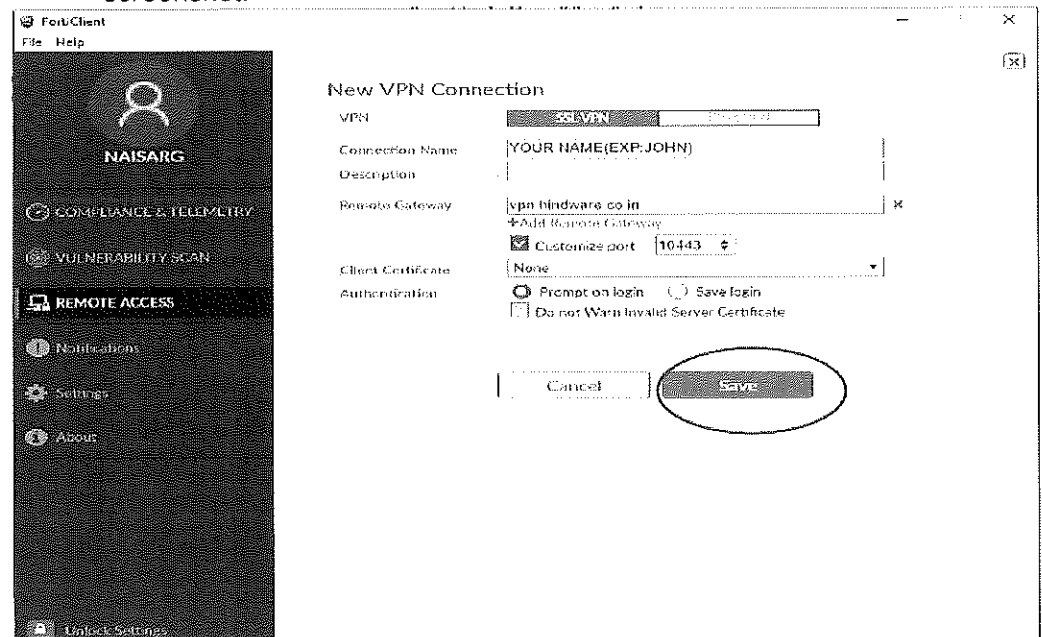
- Every laptop/Desktop installed with End-Point protection. There are two agents at end-point devices. One Agent protects scanned all type of file systems and other agent up to date the antivirus database signatures.
- Through End-Point protection we blocked all systems USB Ports. There is an option to open the USB port allowed permanent, only if requester have approval from respective business CEO and CIO.
- For Temporary short time period access, after receiving approval we allow the USB port with certain time period.

VI. Managing network access and remote access controls:

- Access to the resources on the network is controlled by network access server (Active Directory) to perform authentication and authorization by verifying user's login details. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.
- Remote users access the network using VPN only.
- No changes should be implemented in the network access profile without adequate change control procedures.
- Remote access request from any user must be approved by IT Head/CIO.
- A VPN client is installed on the remote user's desktop recognizes the destination network as a part of remote VPN encryption network.
- **VPN Client Configuration Process:**
- **Step 1:** open the console (software) and click on the remote access. The below screen will open



- **Step 2:** Fill all the details as shown in below screenshot username, remote gateway etc. Select the same settings as selected in below screenshot.



- **Step 3:** Now fill the username and password which provided by IT. And click on connect to connect through VPN.

