

<b>AGI Greenpac Limited</b>		<b>POLICY DOCUMENT</b>	
<b>SUBJECT: Cyber Security Policy</b>			
EFFECTIVE DATE:		POLICY #:	CORP-IT/POLICY/1.0
LAST VERSION DATE	N.A.	LAST VERSION NO.	N.A.
POLICY OWNERSHIP		PROCESS OWNERS: Mr. Prashant Kunjir	
APPLICABILITY OF POLICY		Group Level	

## Contents

1) PURPOSE .....	2
2) Cyber Security – In-Place .....	2
3) Password Policy .....	3
4) Access Control.....	3
5) IT Asset Mgmt & BYOD .....	3
6) Network and Wi-Fi Access .....	4
7) Cloud & On-Prem App Use.....	4
8) IT Software Management .....	5
9) BCP and DR.....	5
10) Cyber Security Roadmap.....	5

<b>AGI Greenpac Limited</b>		<b>POLICY DOCUMENT</b>	
SUBJECT: Cyber Security Policy			
EFFECTIVE DATE:		POLICY #:	CORP-IT/POLICY/1.0
LAST VERSION DATE	N.A.	LAST VERSION NO.	N.A.
POLICY OWNERSHIP		PROCESS OWNERS: Mr. Prashant Kunjir	
APPLICABILITY OF POLICY		Group Level	

## 1) PURPOSE

The main purpose of Cyber Security is to protect all Organizational Assets from both external and internal threats as well as disruptions caused due to natural disasters.

The core functions: identify, protect, detect, respond and recover; aid organizations in their effort to spot, manage and counter cybersecurity events promptly.

As organizational assets are made up of multiple disparate systems, an effective and efficient cyber security posture requires coordinated efforts across all its information systems.

## 2) Cyber Security – In-Place

- We have initiated and establish the roadmap to address Cyber risk areas across the Organization
- Cyber Security framework to address the critical risks identified
- We are operating the automated alerting systems protections control to enhance the cyber resilience
- Third party vendor monitoring the cyber incidents
- We have in place Security policy and processes,
  - Cyber Awareness Program,
  - Security architecture,
  - Access Management (Active Directory and Azure AD),
  - End-Point Protection,
  - Vulnerability assessment,
  - Security Baseline,
  - Firewall Configuration,
  - Isolate OT Network,
  - Secure IT Network (IP-Sec),
  - Application Security,
  - BCP and DR,
  - Security Patch Management,
  - Asset Management
  - Identity Management
- In-Progress of Cyber Security Area,
  - Cyber Simulation,

<b>AGI Greenpac Limited</b>		<b>POLICY DOCUMENT</b>	
<b>SUBJECT: Cyber Security Policy</b>			
EFFECTIVE DATE:		POLICY #:	CORP-IT/POLICY/1.0
LAST VERSION DATE	N.A.	LAST VERSION NO.	N.A.
POLICY OWNERSHIP	PROCESS OWNERS: Mr. Prashant Kunjir		
APPLICABILITY OF POLICY	Group Level		

- Privileged Access Management,
- Software Deployment,
- Access Control,
- Log Management,
- Data Leakage Prevention,
- SOC Management
- Resident Cyber Security Consultant

### 3) Password Policy

- We have setup complexity rules to increase the privacy and security
- Validity for passwords set to 90 days
- Min and Max characters
- At least two special characters
- User must change the default password during initial login
- Number of passwords to keep in history
- Some known passwords will not allow to keep

### 4) Access Control

- Data security process that enables organizations to manage who is authorized to access the data and resources.
- We have secure access control uses policies that verify users are who they claim to be and ensures appropriate control access levels are granted to users
- We are using three types of access control in our systems – DAC, RBAC, & ABAC

### 5) IT Asset Mgmt. & BYOD

- We issue the IT Asset (Laptop/Desktop/Printer/Network Devices/Accessories) having process through IT Asset Management control through SAP. The same process while due receiving the assets from employees

SUBJECT: Cyber Security Policy

EFFECTIVE DATE:		POLICY #:	CORP-IT/POLICY/1.0
LAST VERSION DATE	N.A.	LAST VERSION NO.	N.A.
POLICY OWNERSHIP	PROCESS OWNERS: Mr. Prashant Kunjir		
APPLICABILITY OF POLICY	Group Level		

- For Laptop/Desktop we integrate with Active Directory, Setup VPN, Install allowed software applications, Install end-point protection
- We do not allow any personal device in our network. In case of third party vendor/partner, we have approval process. Once approve from CIO, we provide VPN access and only to specific resource for specific time period.
- Installation protection policy applied on Active Directory GPO
- USB restricted policy applied on all systems using End-Point Protection

### 6) Network and Wi-Fi Access

- We have IT Network and OT Network setup separately
- Site to Site IP-Sec tunnel created to DataCenter
- VPN Tunnel configured from Azure Cloud to Individual sites
- DHCP, DNS, RAS Server setup for our IT Network
- MAC ID Binding to IT Network
- NPS setup for Wifi network
- Separate Guest access network
- Firewall role based policy
- SD-WAN security features enabled on Firewall level
- Allowing only secure and authorized web address

### 7) Cloud & On-Prem App Use

- WAF enabled on all Public access cloud applications
- Remedial actions are automated
- Cloud hosted applications enabled three layer of Security
- On-Prem application in process of SSO integration with On-Premise Active Directory
- Cloud Applications will be integrated with Azure AD for SSO
- All public hosted applications are SSL enabled

<b>AGI Greenpac Limited</b>		<b>POLICY DOCUMENT</b>	
SUBJECT: Cyber Security Policy			
EFFECTIVE DATE:		POLICY #:	CORP-IT/POLICY/1.0
LAST VERSION DATE	N.A.	LAST VERSION NO.	N.A.
POLICY OWNERSHIP		PROCESS OWNERS: Mr. Prashant Kunjir	
APPLICABILITY OF POLICY		Group Level	

- Validation of IT Security before hosting applications

**8) IT Software Management**

- Only compliance software will be allowed to install at the end point devices
- Patch management process followed to update the security updates
- Software security vulnerability taken care through our distribution point
- Centralized software/patch deployment tool is being planned

**9) BCP and DR**

Business Continuity Plan is the practice of maintaining normal operations during unfavourable circumstances, while Disaster Recovery is the process of restoring technology and systems as quickly as possible after an incident

- BCP and DR policies are in place
- Frequent drills will be conducted for priority applications
- On premise, first backup goes to disks and next goes to tape. Tapes transported to offsite locations from the DataCenter. Retention period 1 year and offsite retention 5 years
- Cloud resources backup enabled for all the systems and availability set to 1 month

**10) Cyber Security Roadmap**

**In-Process of Adherence: -**

- Resident Cyber Security Consultant
- Security Governance
- Proper Security Architecture
- DLP
- SSO for On-prem and Cloud Apps

SUBJECT: Cyber Security Policy

EFFECTIVE DATE:		POLICY #:	CORP-IT/POLICY/1.0
LAST VERSION DATE	N.A.	LAST VERSION NO.	N.A.
POLICY OWNERSHIP	PROCESS OWNERS: Mr. Prashant Kunjir		
APPLICABILITY OF POLICY	Group Level		

- PAM
- Cyber Simulation (Phishing)
- Cyber Resilience
- Log/SIEM
- SOC Management

**Future Action Plan:** -

- Threat hunting
- Zero Trust Architecture
- Legal & Compliance Management – Governance framework and Metrics
- Monthly reports on Cyber
- GDPR Compliance

**11) Process Owner**

IT Infrastructure Lead takes the responsibility of process defined

PROCESS / DATA	ROLE	DEPARTMENT
RESPONSIBILITY	INITIATOR	Mr. Prashant Kunjir
ACCOUNTABILITY	APPROVER	Mr. Anjaiah Surgi
OWNERSHIP	DATA CREATOR	IT DEPARTMENT

POLICY REVIEWED BY:		POLICY APPROVED BY:	
Name:	Mr. Prashant Kunjir	Name:	Anjaiah Surgi
Designation:	Senior Manager	Designation:	Sr. Vice President IT (CIO)
Department:	Information Technology	Department:	Information Technology
Date:	25/04/2024	Date:	25/04/2024