BANNARI AMMAN SUGARS LIMITED

Cyber Security Policy

The Cyber Security Policy is to safeguard the interest of organization's stakeholders, customers, business partners and employees and also to comply with the statutory & regulatory requirements. A cyber security framework compromising of the security policies and procedures adopted to effectively protect data/information and assets of the organization and its stakeholders from security threats, whether internal or external, deliberate, or accidental.

Objective

This Information Security Policy addresses:

Confidentiality: Protecting sensitive information from disclosure to unauthorised individuals or systems;
Integrity: Safeguarding the accuracy, completeness, and timeliness of information;

Availability: Ensuring that information and vital services are accessible to authorised users when required;
Compliance: To ensure compliance of legal, regulatory, and contractual requirements

Policy brief & purpose

BASL protects all Information from unauthorized access, use, disclosure, modification, disposal, or impairment whether intentional or unintentional, through appropriate technical and organizational security measures

BASL committed to provide a virus free network and all Information processing systems will be auto updated with latest security patches from the manufacturer and loaded with an approved antivirus system.

BASL provides framework to manage and handle security breaches, violations and business disruptions.

A comprehensive backup procedure is being implemented to protect the business transactions. Backup devices are to be verified by restoring the data for integrity. Backups of the transactional data to be taken thrice in a day. Offline backups taken weekly, monthly and yearly basis.

Only authorized and licensed software will be allowed to be installed on corporate systems.

BASL's network will be always protected from the Internet through a firewall.

All information assets used in production will have either warranty or a support contract from the authorized vendor/ partner

Secure IT Architecture

All servers to be located in a secured area with restricted access.

Firewalls, Internet Gateway, Mail Gateway, DNS servers, Routers & Switches etc. shall have secure configuration and shall be part of continuous surveillance.

BASL shall deploy Antivirus, Anti-malware solution to cover all computing devices.

Removable Media is not permitted to be connected on BASL's networked computers. In case of business requirement, specific permissions required

IT department shall implement system related controls such as disabling of USB ports, controlling of internet access etc., through end point solutions.

Inventory Management of IT Assets

Complete inventory of IT assets shall be maintained with hardware, Software, version numbers, current state of deployment (e.g. what software is installed on what systems) to be maintained

IT Head shall ensure enterprise architecture is defined, developed and periodically reviewed so that manual and administrative controls can be converted into automated one especially end-point control, license compliance, patch management, access control, contract management and performance management.

Protect personal and company devices

When employees use their digital devices to access BASL emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company issued computer, tablet and cell phone secure as:

Keep all devices password protected.

Choose and upgrade complete antivirus software.

Ensure they do not leave their devices exposed or unattended.

Install security updates of browsers and systems monthly or as soon as updates are available.

Log into BASL accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

Keep emails safe

E-mail service authorized by BASL should only be used for official correspondence.
All incoming SMTP e-mails will be scanned for spam and virus infection.

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")

Be suspicious of clickbait titles (e.g. offering prizes, advice.)

Check email and names of people they received a message from to ensure they are legitimate.

Filtering and blocking of sites

IT Department may block content over the Internet which is in contravention of this policy and other applicable laws of the land in force which may pose a security threat to the network.

IT Department may also block content which, in the opinion of the organization concerned, is inappropriate or may adversely affect the network security and productivity of the users/organization.

Network Level Security

BASL network at all levels (LAN, WAN) shall be designed in such a way that no foreign computing resources shall be automatically connected.

All temporary connections to external agencies within BASL or from outside using VPN shall be through strict rules.

Host to Host connectivity shall only be based on a specific requirement

Database Level Security

Database access for each critical application and process through proper authentication mechanism only. Access rights assigned for users as per the requirements and limited for their roles / departments only.

Preventing execution of unauthorised software

End users not allowed to install or uninstall any software (licensed, unlicensed, evaluation version, shareware & freeware) on operational system.

IT support team is responsible for installation or un-installation of all software from operational system

Physical Security and Environmental Controls

Data Centre is regularly maintained to ensure compliance of environmental parameters viz., Power, Air Conditioning, Fire proofing and cleanliness. Room temperature sensor also implemented.

All IT Assets shall ensure minimum level of environment parameters as required by OEMs of respective assets are implemented and maintained. Performance shall be assessed periodically through preventive maintenance.

Physical Access to BASL's Data Centre and other server hosted locations shall be restricted.

All Critical Locations shall be covered through CCTV systems and such footage shall be stored for a minimum period of 1 month.

Application Security

All Critical applications shall follow principles of secure development, segregation of duties, Application Security, Source Code security etc.

Creating Awareness

We shall coordinate to create awareness about Cyber Security amongst employees, Customers, vendors, and Visitors and others using SMS, Email and intranet.

Internet Access

Devices with direct Internet access (which bypass the firewall security) are not allowed to connect to BASL's network and user end points.

Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

Turn off their screens and lock their devices when leaving their desks.

Report stolen or damaged equipment as soon as possible

Change all account passwords at once when a device is stolen.

Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.

Avoid accessing suspicious websites.

* * * * *