**ACCEPTABLE USE POLICY**

**PURPOSE:**

The primary aim of our company's Acceptable Use Policy is to establish guidelines for the responsible and secure utilization of our Information Resources. This is crucial for safeguarding the confidentiality, integrity, and availability of information within our organization.

**AUDIENCE:**

This policy applies to all individuals, entities, or processes that engage with any of our Information Resources.

**CONTENTS:**

1. Acceptable Use
2. Access Management
3. Authentication/Passwords
4. Clear Desk / Clear Screen
5. Data Security
6. Email and Electronic Communication
7. Hardware and Software
8. Internet
9. Mobile Devices and Bring Your Own Device (BYOD)
10. Physical Security
11. Privacy
12. Removable Media
13. Security Training and Awareness
14. Social Media

**POLICY:**

Acceptable Use:

* Comply with (Company) policies while using Information Resources or during company time. Seek assistance from the Information Security Committee for any unclear requirements or responsibilities.
* Promptly report harmful events or policy violations related to (Company) assets or information to a manager or the Incident Handling Team, including technology incidents, data incidents, unauthorized access incidents, facility security incidents, and policy violations.
* Avoid engaging in activities that harass, threaten, impersonate, abuse others, degrade the performance of (Company) Information Resources, deprive authorized personnel access, obtain unauthorized resources, or circumvent computer security measures.
* Do not download, install, or run security programs or utilities that exploit weaknesses in system security, such as password cracking programs, packet sniffers, or port scanners, without approval.

Access Management:

* Access to information is granted based on a "need to know" principle.
* Personnel may use only assigned network and host addresses from (Company) IT and must not attempt unauthorized access to data or programs on (Company) systems.
* All remote access to internal networks must be made through approved (Company)-provided virtual private networks (VPNs).
* Personal authentication information, including passwords, PINs, security tokens, multi-factor authentication details, access cards, keys, and digital certificates, must not be shared.

Passwords/ Authentication:

* Maintain the confidentiality of personal authentication information.
* Keep group/shared authentication information limited to authorized group members.
* Use unique passwords for each system when possible.
* Construct and implement passwords according to (Company) rules, meeting length, complexity, and reuse history requirements.

Clear Desk/ Clear Screen:

* Log off from applications and network services when not in use.
* Lock or log off workstations and laptops when unattended.
* Secure confidential information in locked drawers or cabinets when not at the workstation.
* Lock laptops with cables or store them securely when unattended, especially if not encrypted.

Data Security:

* Use approved encrypted communication methods for sending confidential information over the Internet.
* Secure confidential information sent via USPS or other mail services in line with the Information Classification and Management Policy.
* Handle, transfer, save, and destroy information based on its sensitivity, following appropriate guidelines.

Email and Electronic Communication:

* Prohibit auto-forwarding electronic messages outside (Company) internal systems.
* Ensure electronic communications accurately represent the originator and (Company).
* Do not share accounts without prior authorization from (Company) IT, except for calendars and related calendaring functions.

Software and Hardware:

* Obtain formal approval from IT Management before connecting any hardware to (Company) networks.
* Ensure software installed on (Company) equipment is approved by IT Management and installed by (Company) IT personnel.
* Physically secure all (Company) assets taken off-site at all times.

Internet:

* Do not use the Internet to communicate (Company) confidential or internal information unless confidentiality, integrity, and recipient identity are ensured.
* Utilize the Internet with (Company) networking or computing resources exclusively for business-related activities, avoiding unapproved activities like recreational games, streaming media, or unauthorized network entry
* Adhere to the same policies when accessing the Internet from outside (Company) network using a (Company) owned computer as those within (Company) facilities.

Mobile Devices and Bring Your Own Device (BYOD):

* Personally owned mobile devices can connect to the (Company) network only with formal approval from IT Management, and it's a privilege for employees.
* Personally owned laptops/workstations must have approved virus protection, spyware detection, and an active personal firewall.
* Theft or loss of a mobile device used for (Company) information must be reported immediately, and devices must adhere to encryption standards for storing confidential information.

Physical Security:

* Recording devices, including cameras in mobile devices, are prohibited in secure areas.
* Personnel must consistently display their photo ID access card while inside the building
* Access-controlled areas require personnel to badge in and out, with strict prohibitions on activities like piggy-backing and door propping to circumvent controls.

Privacy:

* Information on (Company) Information Resources is not private and can be accessed by (Company) IT employees under executive management or Human Resources direction.
* (Company) has the right to log, review, and utilize any information stored on its Information Resource systems.
* Personnel with extended privileges should only access information necessary for employment-related tasks.

Removable Media:

* Removable media usage for (Company) information requires a justified business case and prior approval from (Company) IT.
* Personally owned removable media is prohibited for storing (Company) information.
* Loss or theft of removable media containing (Company) information must be promptly reported to (Company) IT.

Security Training and Awareness:

* New personnel must undergo security awareness training before accessing (Company) Information Resources.
* All personnel must acknowledge and adhere to (Company) Information Security Policies before gaining access.
* Annual security awareness training is mandatory for all personnel.

Social Media:

* Social media communications must comply with all relevant (Company) policies.
* Personnel are individually responsible for the content they publish online.
* Permission from the (Company) Communications Department is required for creating public social media accounts representing (Company)

ENFORCEMENT:

Individuals breaching this policy may face consequences ranging from disciplinary measures, including potential job termination, to legal penalties. Similarly, vendors, consultants, or contractors violating this policy may encounter sanctions such as access revocation, contract termination, and legal repercussions.