TEKBOOX IT, ELECTRONIC COMMUNICATIONS & INFORMATION SECURITY POLICY

1. PURPOSE

The purpose of this policy is to establish clear rules for the appropriate, secure, and responsible use of TekBoox information technology resources, electronic communications, company accounts, internet services, software, devices, and digital information.

The policy is intended to protect the Company's confidential information, systems, employees, clients, and business operations from unauthorized access, misuse, disclosure, loss, or security threats.

2. SCOPE

This policy applies to all employees and authorized users who access or use any Company-owned or Company-provided:

- Computers and laptops
- Company email accounts
- Slack and other workplace communication platforms
- Internet and network facilities
- Flow HCM and other Company systems
- Company databases and digital files
- Company-provided mobile devices
- Software and applications
- Cloud services
- Other Company information systems and electronic resources

This policy applies whether Company resources are accessed from Company premises, remotely, through Company-owned equipment, or through Company-paid services.

3. OFFICIAL USE OF COMPANY RESOURCES

Company IT resources, internet facilities, software, systems, electronic communications, databases, hardware, and digital files are provided primarily for official business purposes.

Employees are required to:

- Use Company systems responsibly and professionally.
- Protect Company information from unauthorized access or disclosure.
- Follow all IT, confidentiality, information-security, and workplace policies.
- Use Company resources only for legitimate business purposes.

- Immediately report suspected security incidents, unauthorized access, lost devices, or accidental disclosure of information to IT/Management.

Personal or unauthorized use of Company resources may be restricted or prohibited depending on the nature and impact of the activity.

4. INTERNET AND WEBSITE USAGE

Company internet facilities are intended primarily for official business purposes.

Employees must not access websites or online services that:

- Are illegal or violate Company policy.
- Contain inappropriate, obscene, discriminatory, or offensive material.
- Create a security risk to Company systems.
- Are unrelated to legitimate business requirements where such access is restricted by Management or IT.
- Involve unauthorized downloading, installation, or distribution of software or files.

Social media and other non-business websites may not be accessed through Company internet facilities were prohibited by Management or IT.

The Company reserves the right to restrict or block access to websites, applications, or services that may create security, productivity, legal, or operational risks.

5. COMPANY EMAIL ACCOUNTS AND PASSWORD SECURITY

Company-provided email accounts are Company assets and must be used only for authorized business purposes.

5.1 Password Confidentiality

Employees must keep Company email passwords and all other system credentials strictly confidential.

Employees are strictly prohibited from sharing, disclosing, forwarding, communicating, or providing their Company email passwords to another employee or any third party.

Company email passwords may only be disclosed under exceptional circumstances where:

1. There is a genuine business or technical requirement; and
2. Specific approval has been obtained from authorized Management and/or IT.

Any approved access must be limited to the minimum period and level of access required.

Employees must never share passwords through:

- Slack
- Email
- WhatsApp
- SMS/Text Messages
- Written notes
- Personal messaging applications
- Any other communication channels

Where technical access is required, IT should use appropriate administrative, recovery, or account-management procedures rather than requesting an employee's password.

6. SLACK AND INTERNAL COMMUNICATION PLATFORMS

Slack and other Company-approved communication platforms are official business communication tools and must be used professionally and responsibly.

6.1 Slack Account Security

Employees must:

- Keep Slack passwords and login credentials confidential.
- Never share their Slack password with another employee or third party.
- Never use another employee's Slack account or credentials without authorization.
- Never provide access to the Company's Slack workspace to an unauthorized person.
- Immediately report suspected unauthorized access to IT/Management.

Sharing Slack passwords is strictly prohibited except where specifically approved by authorized Management under exceptional circumstances.

Where access to an employee's Slack account is required for business continuity, IT/Management should use appropriate administrative access procedures rather than obtaining or sharing the employee's password.

6.2 Prohibition on Sharing Credentials Through Slack

Employees are strictly prohibited from sharing their login credentials, passwords, portal passwords, system credentials, or authentication information through Slack.

This includes passwords or credentials for:

- Company email
- Flow HCM
- Client portals
- Internal systems
- Administrative portals
- Cloud applications
- Third-party business systems
- Any other Company-assigned account

If another employee requires access to a system, the appropriate access-request or IT process must be followed.

7. SLACK ON MOBILE PHONES

Slack mobile access is restricted due to information-security and confidentiality requirements.

Slack may only be installed and used on mobile phones by Managers and Leads who have been specifically authorized by Management.

General employees are **not permitted to install, log in to, or use the Company's Slack account on personal mobile phones or other personal mobile devices.**

Where mobile Slack access has been authorized for Managers or Leads, the Company may require:

- Device PIN/password protection.
- Multi-factor authentication.
- Appropriate device security controls.
- Immediate reporting of lost or stolen devices.
- Removal of Company access when authorization is withdrawn.
- Compliance with all Company confidentiality and security requirements.

Company Slack information must not be copied, forwarded, downloaded, photographed, screen-recorded, or transferred to unauthorized personal applications or devices.

8. ACCESS TO OTHER EMPLOYEES' ACCOUNTS

Employees must not access, attempt to access, monitor, copy, modify, or use another employee's:

- Email account
- Slack account
- Flow HCM account
- Computer or workstation
- Files or folders
- Passwords or credentials
- Digital communications
- Company systems

unless specifically authorized by Management or IT for a legitimate business requirement.

Authorization must be limited to the required purpose and scope.

Authorization to access an account does not automatically authorize the sharing of that account's password.

Where possible, IT must provide authorized access through administrative controls rather than sharing the account holder's credentials.

9. PASSWORD AND CREDENTIAL MANAGEMENT

All employees are responsible for protecting their assigned credentials.

Employees must:

- Use strong and unique passwords where required.
- Keep passwords confidential.
- Never share passwords with other employees unless specifically authorized under this policy.
- Never write passwords in publicly accessible locations.
- Never store passwords in unsecured files or notes.
- Never use another employee's credentials.
- Follow Company requirements for multi-factor authentication.
- Change passwords immediately when instructed by IT or when compromise is suspected.

Employees must immediately notify IT/Management if they believe their credentials have been compromised.

10. SCREEN LOCK REQUIREMENT

Employees are required to lock their computer screen whenever they leave their workstation, even for a short period.

Employees must use the appropriate screen-lock function before leaving their system unattended.

Employees must never leave an unlocked Company computer unattended.

This requirement applies to all Company computers, laptops, and other systems containing Company information.

Failure to lock an unattended workstation may be treated as a violation of this IT Security Policy.

11. SOFTWARE INSTALLATION AND IT TICKETS

Employees are **not permitted to install software, applications, browser extensions, tools, or other programs on Company computers or systems without authorization.**

If an employee requires any software or application for business purposes:

1. The employee must generate an IT ticket/request.
2. The requested software must be reviewed and approved by the authorized IT team.
3. An authorized IT team member will install the software if approved.
4. Employees must not attempt to bypass IT controls or install the software themselves.

Only approved and properly licensed software may be installed or used on Company equipment.

Unauthorized software installation may result in disciplinary action.

12. COMPANY DEVICES AND PERSONAL LAPTOPS

Company-provided computers and electronic equipment remain the property of TekBoox and must be used responsibly.

Employees are not permitted to:

- Install unauthorized or personal software on Company computers.
- Disable security controls, antivirus, monitoring, or other protective measures.
- Connect unauthorized devices or storage media where prohibited.
- Use Company systems to download unauthorized or illegal material.
- Bring personal computers/laptops into the office for routine work.

12.1 Personal Laptops

Personal laptops are not permitted on any Company office floor.

Employees must not bring or use personal laptops within Company office areas.

In an exceptional emergency where an employee is required to bring a personal laptop:

- Prior approval should be obtained where possible.
- The personal laptop must be submitted to the **HR Office** upon arrival.
- The employee must inform HR/Management of the reason for bringing the device.
- The device must not be used on the office floor unless specifically authorized by Management.

This restriction is intended to protect Company data, systems, network security, and confidentiality.

13. CONFIDENTIAL AND SENSITIVE INFORMATION

Employees must protect all confidential and sensitive Company information.

Confidential information includes, but is not limited to:

- Employee information
- Payroll and salary information
- Client information
- Financial information
- Business plans
- Contracts and agreements
- Passwords and credentials
- Company databases
- Source code and technical information
- Internal communications
- Trade secrets
- Documents and files marked confidential

Confidential information must not be shared through personal email accounts, personal cloud storage, unauthorized messaging applications, personal devices, or any other unauthorized platform.

14. SUSPICIOUS LINKS, SPAM AND PHISHING EMAILS

Employees must exercise caution when receiving suspicious emails, links, attachments, or messages.

Employees must **not click, open, download, reply to, or provide credentials through suspicious links or emails** unless their legitimacy has been confirmed.

Examples include:

- Suspicious email links
- Unknown attachments
- Fake login pages
- Unexpected password-reset requests
- Emails requesting confidential information
- Unusual payment requests
- Messages from unknown senders
- Suspected phishing emails
- Spam or malicious communications

Employees must generate an IT ticket and report suspicious links, spam, phishing emails, or other potentially malicious communications to IT for review and appropriate resolution.

Employees should not attempt to investigate or resolve suspected malicious emails independently if doing so could create a security risk.

15. MONITORING AND PRIVACY

The Company reserves the right, subject to applicable law and Company procedures, to monitor, access, review, preserve, and investigate the use of Company systems and electronic communications where reasonably necessary for:

- Security purposes
- Business continuity
- Compliance
- Investigation of suspected misconduct
- Protection of Company assets
- Prevention of unauthorized access
- Legal or regulatory requirements

Employees should not assume that information created, stored, transmitted, or processed through Company systems is private.

16. SOFTWARE AND APPLICATION INSTALLATION

Employees may not install software, applications, browser extensions, encryption tools, communication platforms, or other programs on Company systems without appropriate authorization.

Only approved and properly licensed software may be installed or used on Company equipment.

All software requirements must be submitted through the designated IT ticket/request process.

17. INFORMATION SHARING AND DATA TRANSFER

Employees must not transfer Company information to:

- Personal email accounts
- Personal devices
- Unauthorized cloud services
- External storage
- Personal messaging applications
- Unauthorized third-party applications

without prior authorization.

Employees must exercise particular care when sending emails or messages containing confidential information and must verify recipients before sending.

18. SECURITY INCIDENTS

Employees must immediately report any suspected or actual:

- Password compromise
- Unauthorized login
- Data breach
- Phishing attempt
- Malware infection
- Lost or stolen Company device
- Unauthorized sharing of Company information
- Unauthorized access to Company systems
- Accidental disclosure of confidential information

to IT/Management through the appropriate reporting process.

Employees must not attempt to conceal, delete, or manipulate evidence relating to a suspected security incident.

19. EMPLOYEE RESPONSIBILITIES

Every employee is responsible for:

1. Protecting Company systems and information.
2. Maintaining the confidentiality of assigned credentials.
3. Locking their computer whenever leaving their workstation.
4. Following IT and information-security instructions.
5. Using Company resources only for authorized purposes.
6. Reporting security incidents immediately.
7. Generating IT tickets for software installation and security concerns.
8. Not sharing credentials through Slack or other communication platforms.
9. Not installing unauthorized software.
10. Not bringing personal laptops onto Company office floors.
11. Cooperating with authorized investigations.
12. Ensuring Company information is not disclosed to unauthorized persons.

20. MANAGEMENT AND IT AUTHORITY

The Company reserves the right to:

- Modify or update this policy as required.
- Restrict access to systems or applications.
- Suspend or terminate user access where a security or business risk exists.
- Reset or disable accounts.
- Review system activity where permitted by law.
- Retrieve Company information required for business continuity.
- Implement additional security controls.
- Require employees to comply with new security procedures.
- Remove unauthorized software or applications from Company systems.
- Restrict mobile access to Company systems.

21. POLICY VIOLATIONS

Violation of this policy may result in disciplinary action depending on the nature and severity of the violation.

Disciplinary action may include:

- Verbal or written warning
- Suspension of system access
- Formal disciplinary action
- Recovery of losses or costs where applicable
- Suspension or termination of employment
- Legal action where appropriate

Serious violations, including but not limited to:

- Intentional disclosure of passwords
- Sharing Company email or Slack passwords without authorization

- Sharing credentials through Slack
- Unauthorized access to Company accounts
- Unauthorized software installation
- Deliberately bypassing security controls
- Unauthorized sharing of confidential information
- Using unauthorized personal devices to access Company information
- Deliberately ignoring security requirements

may result in severe disciplinary action, up to and including termination of employment.

22. SEPARATION FROM THE COMPANY

Upon resignation, termination, or completion of employment/contract, all Company accounts, systems, devices, files, documents, credentials, and information must be returned or surrendered as instructed by Management/IT.

Employees must not retain, copy, transfer, or use Company information or credentials after their access has been withdrawn.

IT/Management may immediately disable or modify access to Company systems when employment or authorization ends.

23. POLICY ACKNOWLEDGMENT

All employees are required to read, understand, and comply with this policy.

By accessing or using Company IT resources, employees acknowledge that they are responsible for protecting Company information and following the requirements of this policy.

Failure to comply with this policy may result in disciplinary action.

The Company may revise this policy from time to time based on operational, technological, legal, or security requirements.