Document 9: IT Usage and Security Policies

Technology and information are central to our work, and it's crucial that all employees use company IT resources responsibly and securely. This document describes the policies for **use of company equipment, internet and email**, data security, and general IT guidelines. By following these policies, you help protect not only our company's sensitive data but also your own privacy and the smooth functioning of our tech systems.

Use of Company Equipment: We provide you with the necessary equipment (such as a laptop, monitor, phone, or other devices) to perform your job. All **company equipment** is to be used primarily for business purposes. You should not install any unauthorized software or hardware on your company devices. If you need a particular software, request it from IT – they will ensure it's properly licensed and safe. Treat the equipment with care: don't leave laptops unattended in public places, avoid eating/drinking over your keyboard to prevent damage, etc. If any equipment is lost, stolen, or damaged, report it to IT immediately. You may be asked to file a police report if theft is involved. **Personal use** of company devices (like checking personal email or doing a quick personal task) is allowed in moderation, but it should be limited and never conflict with work responsibilities. All data on company devices is considered company property, and the company reserves the right to access or monitor it in accordance with law and policy (for example, if troubleshooting an issue or investigating a security incident).

Internet and Email Usage: Our **internet policy** expects you to use good judgment. Do not use the company network to visit inappropriate websites (such as those containing pornography, hate speech, or illegal content). Web filtering is in place to block many inappropriate sites. **Email** should be used for business communications. Be cautious with personal email use on company systems – it can introduce security risks. Phishing attacks (malicious emails) are common; do not click suspicious links or open unexpected attachments. Our IT team will never ask for your password via email. We periodically send out simulated phishing tests to keep everyone vigilant. Always follow email etiquette: use a professional tone and only CC people who need to be in the conversation. The company also has access to emails on our servers, so never put something in email that you wouldn't want associated with work. Keep personal correspondence on personal devices/accounts.

Password and Account Security: You will receive various login accounts (computer login, email, etc.). It's vital to maintain strong security for these accounts. **Use strong passwords** – at least 8 characters with a mix of letters (upper and lower case), numbers, and symbols. Even better, use a passphrase (a sentence-like string of words). Do not reuse your company password on any other site. We enforce password changes every 90 days for key accounts. Additionally, we use **Multi-Factor Authentication (MFA)** for remote access and important applications, meaning you'll need a second step (like a code from an authenticator app or text message) when logging in. Never share your passwords with anyone, not even IT. If someone needs access to something, IT can grant it without you giving out credentials. If you suspect any

account compromise (e.g., you accidentally entered your password on a phishing site), report it to IT immediately so we can secure the account.

Data Protection and Privacy: Depending on your role, you might handle sensitive data – like customer information, financial records, or personal data of employees. Always store such data in approved locations (like company cloud storage or servers) and **not on unapproved personal drives**. Our company systems (like the corporate Google Drive or SharePoint) are secured and backed up; using them ensures data is protected and retrievable. Do not transfer company data to personal email or cloud accounts. **Encryption:** All company laptops are encrypted to protect data in case of loss. Do not attempt to disable security settings on devices. When sharing files externally, use secure methods approved by IT (for example, a protected link rather than an open email attachment, if the data is sensitive). We also require that any personal devices used for work (like if you sometimes read email on your personal phone) be enrolled in our mobile device management (MDM) system, which allows for a remote wipe of company data if the device is lost.

Software and Downloads: Only use software that is approved/licensed for company use. Installing random freeware or clicking “Yes” on unknown downloads can introduce malware. We have anti-virus and anti-malware software running on all systems – do not disable it. If you receive a pop-up or suspect a virus, call IT. Avoid downloading large non-work files (like movies, etc.) on the company network to preserve bandwidth and avoid legal issues. Also, do not engage in illegal downloads or file sharing (torrenting) on company equipment or network – this is against policy and the law.

Use of Personal Devices (BYOD): If you use your **personal phone or tablet** for work purposes (like checking email or Slack), you must abide by our security requirements. This includes having a PIN or biometric lock on your device and agreeing to install a profile that can erase company email if the device is lost. Personal laptops are generally **not** allowed for work use unless specifically authorized, because we cannot ensure they meet our security standards. The company will provide the necessary computer equipment for your role. If you’re remote and have special equipment needs (printer, etc.), talk to IT/HR – we have a policy for expense reimbursement or providing additional peripherals.

IT Support and Issue Reporting: Our IT Help Desk is available to assist with any technical problems or questions. You can reach them by ticket system (helpdesk@ourcompany.com) or phone during business hours. If you encounter any system error, network outage, or other IT issue that affects your work, report it so they can fix it promptly. For after-hours emergencies (like a critical server is down), there’s an on-call procedure posted on the intranet. We aim to respond to critical issues within an hour and normal requests within one business day. Also, periodically, IT will schedule maintenance downtime for system upgrades – these will be communicated in advance via email.

Cybersecurity Awareness: Security is everyone’s responsibility. Be alert for any suspicious activity. This could be unknown people tailgating you through a secure door at the office, unusual emails as mentioned, or finding a USB drive lying around (do **not** plug it in – it could be

malicious; give it to IT). We conduct annual **security awareness training** which is mandatory for all employees. This training covers the latest best practices and company policies regarding data protection. Please complete it by the given deadline each year.

Privacy and Monitoring: Please be aware that while we respect employee privacy, the company retains rights to monitor usage of corporate IT resources in accordance with law and policy. For instance, internet traffic through our network and activity on company devices can be logged. We do this to protect against threats and ensure compliance. We do **not** actively spy on personal communications, but you should have no expectation of complete privacy on work systems. Always use work devices and networks with the understanding that they are primarily for professional use.

Social Engineering and Scams: Not all security threats are technical – some are social. Never give out confidential information to someone who calls or emails you out of the blue claiming to be from IT or management without verifying their identity. If someone asks for sensitive info, double-check. For example, if “IT” calls asking for your password – that’s a red flag (IT will never do that). If HR emails requesting personal info that seems odd, verify by calling them. It’s okay to be cautiously paranoid when it comes to security.

Consequences of Policy Violation: Using IT resources inappropriately (such as accessing offensive materials, pirating software/music, or bypassing security controls) or mishandling confidential data is taken seriously. Depending on severity, violations can result in disciplinary action, including possible termination. For example, deliberately disabling security settings or repeatedly falling for phishing due to not following guidelines might trigger corrective action. These measures are not to be punitive, but to protect our entire organization’s security and legal compliance.

By following the above policies, you help us maintain a secure and efficient computing environment. Technology enables us to do great work – let’s use it responsibly. If you have any questions about acceptable use or need an exception to a policy (sometimes needed for specific business reasons), please contact the IT Security team. They will evaluate and approve any necessary exceptions in writing. Thank you for being vigilant and keeping our digital workplace safe!