Data Security and Privacy in the Workplace

Protecting company and personal data is a shared responsibility across the entire organization. Every employee, regardless of position, contributes to maintaining the confidentiality, integrity, and availability of information.

1. Use strong and unique passwords
Create complex passwords that include a mix of letters, numbers, and symbols. Avoid using personal information such as birthdays or names. Change passwords regularly and never share them with others.

2. Be cautious with emails and links
Phishing attacks are one of the most common ways for hackers to gain access to data. Always verify the sender's address and never click on suspicious links or attachments.

3. Lock your devices when unattended
Always lock your computer or phone when leaving your workstation, even for a short time. This prevents unauthorized access to company systems.

4. Handle confidential documents carefully
Do not print or leave sensitive materials on your desk or in shared spaces. Use secure shredders to dispose of old or unnecessary documents.

5. Use secure networks and devices
Avoid connecting to public Wi-Fi when accessing company resources. Always use the corporate VPN and ensure your device has the latest security updates.

6. Report incidents immediately
If you notice suspicious activity, data loss, or potential breaches, report them immediately to the IT or security department. Early reporting minimizes risk and helps contain damage.

7. Maintain awareness and training
Regularly participate in cybersecurity awareness programs. Staying informed about modern threats helps keep company information secure.

Creating a culture of privacy and security not only protects sensitive data but also strengthens trust among employees, customers, and partners.