

Cyber Security Policy

Policy Brief & Purpose

This policy sets out the standard steps for protecting the organization's data, systems and IT infrastructure from cyberattacks. Cloud-based HRMS platforms and remote access tools are now part of everyday work, and every added tool raises the risk of a data breach.

It lists the security measures everyone must follow and the responsibilities that come with using company systems. It protects sensitive HR information such as employee records and payroll data, and supports compliance with privacy laws like the GDPR and the IT Act.

Its main goal is to protect the confidentiality, integrity and availability of data, so that business can run safely and in line with the law.

Scope

This policy applies to all employees, contractors, consultants and third-party vendors who access or use [Name of the Company](#) systems, networks and data, whether they work on-site or remotely.

Confidential Data Protection

Confidential information includes employee records, payroll data, customer information, financial details and any other non-public company data. If it were disclosed without authorization, it could seriously harm the company, its employees or its stakeholders.

- Keep this information confidential and do not disclose it.
- Access confidential data only for authorized, approved business purposes.
- Do not discuss it in public places or while connected to an unsecured network.
- You are responsible for protecting it from unauthorized access, loss and misuse.
- Follow the established security controls and company policies whenever you handle sensitive data.
- Violations can lead to serious disciplinary action, up to termination and legal consequences.

Protect Personal and Company Devices

Using a personal or company device to reach systems, email or HRMS portals puts sensitive company data at risk. Keep every computer, tablet and phone secure by following these rules:

- Protect work devices with strong, complex passwords.
- Install company-approved antivirus and anti-malware software, and keep it updated.
- Keep operating systems, applications and security patches up to date.
- Reach company IT platforms and communication tools only over secure, private networks.
- Never leave a work device unattended or in plain view in a public place.
- Do not access company accounts from public devices, and do not let unauthorized people use a company-authorized device.
- Ask IT Support if you have any question about device security, especially when handling payroll information.

Keep Emails Safe

Emails are a common route for phishing and malware. These rules protect the company network and sensitive information:

1. Use your official company email account only for approved business.
2. Do not share your login details, and do not leave your email open and unattended.
3. Use encryption or a secure messaging platform when sending sensitive information outside the company.
4. Do not open unexpected attachments, click suspicious links or reply to clickbait emails.
5. Always check who sent the email, and watch for signs such as poor grammar or odd email addresses.
6. If you are not sure an email is safe, do not click anything and report it to IT right away.
7. Turn on multi-factor authentication (MFA) for all email and communication accounts.

Manage Passwords Properly

Passwords are the first line of defense for company systems. Follow these rules:

- Create passwords of at least 12 characters that mix uppercase and lowercase letters, numbers and special symbols.
- Change a password immediately after any suspected breach, unauthorized access or accidental sharing.
- Keep passwords confidential. Never write them on sticky notes or store them in unprotected digital files.
- Turn on MFA on every platform that offers it.
- Report any suspected password leak to the IT department immediately.

Transfer Data Securely

Moving data creates openings for interception. To reduce that risk:

- Use only approved transfer methods such as SFTP, encrypted email or the secure company cloud drive.
- Encrypt sensitive files before sending them outside the company.
- Check that recipients are authorized to see the data and follow proper security practices.
- Never use public Wi-Fi to transfer confidential data.
- Do not send sensitive data to personal cloud services or to personal email accounts that have not been approved.

Report Scams, Breaches and Hacking Attempts

If you suspect a scam, data breach or hacking attempt, report it immediately to the IT Security Team or the designated incident response coordinator. Reporting quickly limits the damage.

- Report suspected phishing, malware or unusual system behavior straight away.
- Include useful details, such as the sender, the email content or what unusual behavior you saw.
- Follow the IT team's remediation guidance after you report.
- Cooperate with investigations and support company-wide alerts.

Additional Security Measures

To cut the risk of incidents, follow these everyday habits:

- Lock your computer (for example, Windows key + L) and turn off the screen when you leave your desk.
- Report lost, stolen or damaged devices to IT and HR immediately.
- If a phone or laptop is lost, change all your account passwords right away.
- Do not download or install suspicious, unauthorized or illegal software on a company device.
- Follow the company's social media and internet acceptable use policies at all times.

Remote Employees

Remote employees follow every instruction in this policy exactly as on-site employees do. In addition:

- Access company accounts and data securely from your home location.
- Use the company-provided VPN for all work connections, so data is encrypted in transit.
- Secure your home Wi-Fi with a strong router password and a built-in firewall.
- Ask IT administrators for help setting up a secure remote workstation.

Disciplinary Action

We expect everyone to follow this policy closely. Breaking it puts the business and its reputation at serious risk. Disciplinary action depends on how serious the violation is, whether it was intentional, and the impact it had.

- Unintentional violations: minor mistakes that cause no harm lead to a formal warning and mandatory security training.
- Careless violations: repeatedly ignoring security rules leads to suspension without pay while the incident is investigated.
- Intentional, severe breaches: deliberate sabotage or unauthorized access to confidential data leads to immediate termination of employment.
- Criminal acts: hacking, data theft or fraud will lead to immediate legal proceedings, civil lawsuits and criminal charges.

Disclaimer

This policy template offers general guidelines and should be used as a reference only. It may not account for every relevant local, state or federal law, and it is not a legal document. The author assumes no legal liability that may arise from using it.