Title: NovaSoft IT and Security Policy

1. Passwords

- Passwords must be at least 12 characters long and include letters and numbers.
- The same password must not be reused across multiple company systems.
- Passwords should not be shared with anyone, including IT staff.

2. Devices

- Only company-approved laptops may be used to access production systems.
- Laptops must have disk encryption and company antivirus installed.
- Screens should be locked when stepping away from the desk.

3. VPN and remote access

- Access to internal tools from outside the office requires VPN.
- VPN credentials are provided by the IT team after manager approval.
- Public Wi-Fi should be used only with VPN turned on.

4. Data handling

- Confidential documents should be stored only in approved cloud drives.
- Company data should not be copied to personal email or USB drives.
- Customer data must never be shared outside NovaSoft without a signed agreement.

5. Incident reporting

- Any suspected security incident (lost laptop, phishing email, data leak) must be reported to IT within one hour of discovery.
- Employees should use the “Security-Incident” ticket type in the helpdesk tool.

6. Software installation

- Employees must not install unlicensed or pirated software on company devices.
- For new tools, raise a request to IT for approval and installation.

7. Email and phishing

- Employees should be cautious about unexpected emails asking for passwords, OTPs, or payments.
- Links in suspicious emails should not be clicked; instead, report them to IT for verification.
- The security team may periodically send simulated phishing emails for training purposes.

8. Use of personal devices (BYOD)

- Personal phones and tablets may be used for email and calendars only if they are secured with a lock screen.

- Company data on personal devices must be removed when the employee leaves NovaSoft.
- Storing source code or confidential documents on personal devices is not allowed.

9. Physical security

- Visitors must be registered at reception and accompanied by a NovaSoft employee at all times.
- ID cards should be worn visibly inside the office premises.
- Desks should be cleared of sensitive papers before leaving for the day.

10. Cloud and SaaS applications

- Only approved SaaS tools may be used for storing or sharing company data.
- Free or trial tools that handle confidential information must be reviewed by IT before use.
- Sharing login credentials for SaaS tools between employees is not allowed.

11. Source code repositories

- All project source code must be stored in the company-approved Git hosting platform.
- Direct pushes to the main branch are restricted; pull requests and code reviews are required.
- Access to repositories should follow the principle of least privilege.

12. Security training

- All employees must complete annual security awareness training.
- Specialized training is required for teams that manage infrastructure or handle sensitive customer data.
- Completion status may be part of performance evaluation for relevant roles.

13. Handling lost or stolen devices

- If a laptop or phone with company data is lost or stolen, employees must inform IT immediately.
- IT will attempt to remotely wipe or lock the device if possible.
- A formal incident report may be filed depending on the severity.

14. Policy violations

- Minor, first-time violations may result in a warning and additional training.
- Repeated or serious violations, such as intentional data leakage, may lead to disciplinary action up to and including termination.
- All violations will be reviewed by HR and the security team.