





BEST PRACTICES FOR IT SUPPORT SECURITY

IT support refers to the technical assistance provided to users and organizations to resolve issues related to computer systems, software, hardware, networks, and other technology resources. This support is essential to ensure optimal operation of business processes and employee productivity. It also involves troubleshooting, incident management, configuration and maintenance, cybersecurity, user assistance, asset management, monitoring, and data recovery.

Technical IT support is one of the foundational pillars of any modern organization. However, it also represents a critical security risk, as technicians often have privileged access to systems, sensitive data, and internal networks. Therefore, implementing security best practices in IT support is not optional, it is essential to protect the integrity, confidentiality, and availability of information.

IT support is not just a technical function, it is also a security responsibility. Implementing controls, training staff, and following best practices helps:

-  Prevent unauthorized access
-  Protect company and customer information
-  Ensure compliance with legal regulations
-  Guarantee business continuity



In a software development company, like Netguard Solutions:

The IT Support area plays a critical role not only in keeping systems running, but also in protecting the most valuable digital assets: source code, customer data, and development, testing, and production environments.



How to implement IT support security best practices?



Access Control

- Apply the principle of least privilege: only grant access necessary for each task.
- Implement multi-factor authentication (MFA) on critical systems.
- Avoid sharing credentials between technicians.



Password Management

- Use secure, unique passwords.
- Utilize an approved password manager.
- Change default passwords on new devices or systems.



Updates and Patches

- Keep operating systems and software up to date.
- Apply security patches as soon as they are released.
- Use remote administration tools with centralized update functions.

✓ **Secure Use of Remote Support Tools**

- Use encrypted connections (e.g., RDP with VPN, TeamViewer with verification).
- Request explicit user authorization before connecting.
- Properly end sessions and close remote access when not in use.

✓ **Backup and Recovery**

- Ensure automatic and regular backups are in place.
- Periodically test recovery processes.
- Make sure backups are encrypted and stored separately from the production environment.

✓ **Monitoring and Logging**

- Enable access and activity logs on servers, workstations, and support tools.
- Monitor for suspicious events or unauthorized access.
- Use SIEM or analytics tools where possible.

✓ **Physical Security**

- Control physical access to servers, networks, and workstations.
- Use locks, cameras, or ID cards, depending on the environment.

✓ **Training and Awareness**

- Train technical staff and end-users on phishing, social engineering, and security policies.
- Document safe procedures for common tasks (e.g., installations, remote support).

✓ **Policies and Procedures**

- Define clear support policies (working hours, access limits, response times).
- Log every incident or technical intervention.
Establish defined security incident response procedures.

✓ **Email and Web Security**

- Avoid opening suspicious attachments or links.
- Use antispam filters and up-to-date antivirus.
- Set secure internet and corporate email usage policies.

IT support security is a strategic element in software companies. It goes beyond resolving incidents—it involves protecting critical assets, ensuring development continuity, and securing environments against human errors, cyberattacks, and poor practices.

