# Information Technology (IT) Policy

## 1. Purpose

This policy establishes guidelines for the proper, ethical, and secure use of Information Technology (IT) resources at Ozrit . It aims to protect Ozrit data, ensure compliance with legal requirements, maintain system integrity, and support smooth business operations.

## 2. Scope

This policy applies to:
- All employees, interns, contractors, and third-party vendors.
- All IT resources including computers, laptops, mobile devices, servers, networks, internet services, email systems, applications, cloud platforms, and databases owned or operated by Ozrit.

## 3. Acceptable Use

IT resources must be used solely for business purposes.
- Limited personal use is permitted if it does not:
  - Interfere with work responsibilities.
  - Consume significant system/network resources.
  - Violate Ozrit rules, laws, or ethical standards.
- Prohibited actions include:
  - Accessing, downloading, or distributing offensive, illegal, or harmful material.
  - Installing unauthorized software/applications.
  - Using IT resources for personal financial gain or competing business.

## 4. Data Security & Confidentiality

Employees must protect Ozrit and client data at all times.
- Passwords must be strong, unique, and changed every 60–90 days.
- Data must only be stored on Ozrit-approved devices/servers.
- Confidential or sensitive information must not be shared without authorization.
- External storage (USB drives, HDDs, etc.) requires prior IT approval.
- All employees must comply with data protection and privacy laws applicable to our business.

## 5. Network & System Usage

Employees must not attempt to:
- Disable, bypass, or tamper with firewalls/security controls.
- Access restricted systems without authorization.

Remote connections must use secure channels (VPN or Ozrit-approved tools).
Internet access should be work-related; malicious or unsafe websites must be avoided.
IT reserves the right to restrict or block non-business applications/websites.

## 6. Email & Digital Communication

Ozrit email must be used for official communication only.
Employees must:
- Avoid sharing sensitive information without encryption or approval.
- Refrain from opening suspicious links or attachments.
- Not use personal email for business-related communication.

Professional and respectful communication is mandatory across all digital platforms.

## 7. Software & Licensing

Only IT-approved and properly licensed software may be installed.
- Copying, pirating, or distributing unlicensed software is strictly prohibited.
- Software updates and patches must be installed as directed by the IT team.

## 8. Hardware & Asset Management

All devices provided by the Ozrit remain Ozrit property.
- Employees are responsible for the safe use of issued devices.
- Loss, theft, or damage of Ozrit equipment must be reported immediately.
- Upon separation, employees must return all IT assets, credentials, and access devices.

## 9. Remote Work & BYOD (Bring Your Own Device)

Employees using personal devices for work must:
- Install Ozrit-approved security software.
- Ensure data is encrypted and password-protected.
- Access Ozrit systems only via secure channels.
The Ozrit reserves the right to restrict, monitor, or remove Ozrit data from personal devices in cases of misuse, theft, or non-compliance.

## 10. Monitoring & Compliance

[Ozrit reserves the right to monitor IT systems, including emails, internet usage, and device activity, to ensure compliance.
Any violation of this policy may result in disciplinary action, up to and including termination of employment, and legal action where applicable.
This policy will be reviewed annually and updated as required.

## 11. Incident Reporting

Employees must report immediately any:
- System malfunction or IT failure.
- Data breach, loss, or suspected theft.
- Phishing attempts, malware, or suspicious cyber activity.
Reports should be made to the IT Department or Security Team without delay.

## 12. Policy Acknowledgment

All employees must read, understand, and sign this policy before being granted access to IT systems.
By signing, employees agree to abide by the rules and responsibilities outlined in this document.