CYBERWHIZ SİBER GÜVENLİK A.Ş.
19 Mayıs Mah. 19 Mayıs Cad.
Golden Plaza No:3 İç Kapı No:16
34360 Şişli/İstanbul
Telefon : (0505) 242 35 82
Web-site : www.CyberWhiz.co.uk

Information Security Policy

Organization: CyberWhiz Cyber Security
Document: Information Security Policy

Document Control Information

Version	Date	Author	Reviewed by	Approved by	Remarks
1.0	03.12.2025	CISO (Purple Team Director)	CIO	CEO	Initial release

1. Purpose

The purpose of this policy is to establish CyberWhiz Cyber Security's commitment to protecting information assets and ensuring the confidentiality, integrity, and availability of data within the scope of the Information Security Management System (ISMS).

2. Scope

This policy applies to:
- All employees, contractors, and third parties with access to information assets related to Red Team services.

3. Policy Statement

- Protecting client and company information from unauthorized access, disclosure, alteration, and destruction.

- Complying with all relevant legal, regulatory, and contractual requirements (including KVKK and GDPR).

- Aligning information security objectives with the strategic direction of the company.

- Ensuring all employees and contractors understand their information security responsibilities.

- Implementing appropriate risk management practices to identify, assess, and treat information security risks.

- Establishing, maintaining, and continually improving the ISMS in line with ISO/IEC 27001:2022.

- Promoting awareness and training to foster a strong information security culture.

CYBERWHIZ SİBER GÜVENLİK A.Ş.
19 Mayıs Mah. 19 Mayıs Cad.
Golden Plaza No:3 İç Kapı No:16
34360 Şişli/İstanbul
Telefon : (0505) 242 35 82
Web-site : www.CyberWhiz.co.uk

4. Information Security Objectives

- Ensure 100% of Red Team deliverables are securely stored and encrypted.
- Achieve and maintain full compliance with KVKK and GDPR.
- Ensure all corporate workstations are protected.
- Conduct annual ISMS internal audits and management reviews.
- Reduce security incidents impacting Red Team operations by at least 20% year-over-year.
- Harden information asseets used by Red Team operations.
- Maintain employee awareness of phishing and social engineering threats.
- Ensure all employees confidently promotes confidentiality.

5. Responsibilities

- CEO: Provides strategic direction and approves this policy.
- CISO (Purple Team Director): Accountable for the ISMS and oversees implementation.
- Cloud Security Architect: Ensures technical implementation of controls and compliance.
- All Employees: Responsible for complying with this policy and reporting security incidents.

6. Review and Approval

This policy shall be reviewed annually, or sooner if significant changes occur in business processes, technology, or regulatory requirements.