

Information Security Policy

1. Purpose

The purpose of this Information Security Policy is to protect Oriental's information assets from all threats, whether internal or external, deliberate or accidental. This policy ensures the confidentiality, integrity, and availability of information, in compliance with applicable legal, regulatory, and contractual obligations.

2. Scope

This policy applies to all employees, contractors, consultants, temporary staff, and third-party service providers who access Oriental's information systems or handle data on behalf of the company.

3. Information Security Objectives

- Ensure the confidentiality of customer and company data.
- Protect the integrity and accuracy of information.
- Guarantee availability of information and services.
- Comply with legal and regulatory requirements, including gaming authority standards.
- Promote a culture of security awareness.

4. Roles and Responsibilities

- Information Security Officer (ISO): Oversees implementation of this policy, monitors compliance, and manages incident response.
- Management: Ensures that information security is integrated into business processes and supports security initiatives.
- Employees and Contractors: Must comply with this policy and report any security incidents immediately.

5. Access Control

- Access to systems and data is granted based on the principle of least privilege.
- User accounts are unique, and usage is monitored and logged.
- Multi-factor authentication (MFA) is required for all critical systems.

6. Data Classification and Handling

- Data is classified into public, internal, confidential, and restricted.
- Sensitive data (e.g., personal identification, payment details) must be encrypted in transit and at rest.
- All data must be backed up regularly and stored securely.

7. Network and System Security

- Firewalls, intrusion detection/prevention systems, and anti-malware are deployed across networks.
- Systems are regularly patched and updated to address security vulnerabilities.
- Remote access must be secured using VPNs and encrypted protocols.

8. Physical Security

- Access to data centers and offices is restricted to authorized personnel only.
- Visitor access is logged and monitored.

9. Security Incident Management

- All security incidents must be reported immediately to the ISO.
- Incidents are logged, investigated, and remediated promptly.
- A post-incident review is conducted to prevent recurrence.

10. Business Continuity and Disaster Recovery

- Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs) are maintained and tested regularly.
- Critical data and systems are backed up and redundancies are in place.

11. Compliance and Audit

- Regular internal and external audits are conducted to ensure compliance.
- Non-compliance with this policy may result in disciplinary action.

12. Policy Review and Updates

This policy is reviewed at least annually or whenever significant changes occur in the organization or relevant regulations.

13. Training and Awareness

All staff receive regular training on information security practices and are required to acknowledge understanding of this policy.
