Information Security, Data Privacy and Cybersecurity Policy

OHI Group Corporate Policy

Document Control	
Security Level	Public
Company	OHI Group
Department	CEO Office
Approved By	CEO
Date	July 2026
Revision	1.0

Contents

Information Security, Data Privacy and Cybersecurity Policy **1**

OHI Group Corporate Policy **1**

1. Policy Objectives 3

2. Scope 3

3. Information Security Principles 4

4. OHI Group Security Commitments 4

5. Data Privacy and Protection 5

6. Information Classification and Handling 5

7. Access Control and Identity Management 6

8. Cybersecurity and Technology Protection 6

9. Third-Party and Supplier Security 7

10. Cloud, Digital Transformation and AI Security 7

11. Information Security Awareness and Responsibilities 7

12. Information Security Incident Management 7

13. Business Continuity and Resilience 8

14. Governance and Accountability 8

15. Monitoring, Assurance and Review 8

1. Policy Objectives

Information is one of OHI Group's most valuable business assets.

The ability to protect information, technology systems, operational data, customer information, employee information, and intellectual property is fundamental to maintaining trust with our customers, employees, partners, regulators, and stakeholders.

OHI Group is committed to protecting information through effective security controls, responsible data management, and a risk-based approach to cybersecurity.

This Policy establishes the principles and minimum requirements for safeguarding:
- Confidentiality of information
- Integrity and accuracy of information
- Availability of systems and services

OHI Group recognises that effective information security enables business continuity, operational excellence, innovation, and sustainable growth.

This Policy supports OHI Group's commitment to:
- Responsible digital transformation
- Protection of personal data
- Cyber resilience
- Ethical use of technology
- Compliance with applicable laws and regulations

Including:
- Oman Personal Data Protection Law (Royal Decree 6/2022)
- Applicable GCC data protection requirements
- Customer contractual obligations
- Industry cybersecurity standards

2. Scope

This Policy applies across OHI Group, including all subsidiaries, controlled entities, business units, and operations.

It applies to:
- Employees
- Directors
- Contractors
- Consultants
- Temporary workers
- Suppliers and third parties accessing OHI Group information or systems

Information covered by this Policy includes:
- Employee personal data
- Customer information
- Commercial information
- Financial information
- Project documentation
- Engineering data
- Intellectual property
- Contracts and tenders
- Operational information
- Digital systems and applications

Information must be protected regardless of its format, including:
- Electronic data
- Paper documents
- Emails and communications
- Cloud environments
- Mobile devices
- Verbal discussions

3. Information Security Principles

OHI Group applies three fundamental information security principles:

Confidentiality
Ensuring information is accessible only to authorised individuals and organisations.

Integrity
Ensuring information remains accurate, complete, and protected against unauthorised modification.

Availability
Ensuring authorised users can access information and systems when required to perform their responsibilities.

4. OHI Group Security Commitments

OHI Group is committed to:

Risk-Based Security
Information security risks will be identified, assessed, managed, and monitored according to business impact and risk appetite.

Security by Design
Security considerations will be embedded into:
- New systems
- Digital solutions
- Technology projects
- Software development
- AI solutions
- Business processes

Security must be considered from the beginning, not after implementation.

Protection of Critical Assets
Critical business assets will receive appropriate levels of protection based on:
- Business importance
- Confidentiality requirements
- Operational impact
- Regulatory obligations

Continuous Improvement
OHI Group will continually improve cybersecurity capability through:
- Monitoring
- Testing
- Training
- Lessons learned
- Technology improvements

5. Data Privacy and Protection

OHI Group respects the privacy rights of individuals and is committed to protecting personal information.

Personal data must be:
- Collected lawfully and transparently
- Used only for legitimate purposes
- Protected against unauthorised access or disclosure
- Retained only as long as necessary
- Managed in accordance with applicable legislation

Personal data includes information relating to:
- Employees
- Customers
- Suppliers
- Partners
- Visitors
- Other individuals connected with OHI Group

Employees must ensure personal data is handled responsibly and only accessed where authorised.

6. Information Classification and Handling

OHI Group will classify information according to its sensitivity and business importance.

Information classifications may include:

Public
Information approved for external communication.

Examples:
- Published reports
- Marketing material
- Public announcements

Internal
Information intended for OHI Group employees.

Examples:
- Internal procedures
- Operational information

Confidential
Sensitive information requiring controlled access.

Examples:
- Contracts
- Commercial information
- Customer information
- Employee records

Restricted
Highly sensitive information requiring enhanced protection.

Examples:
- Strategic information
- Security credentials
- Critical operational data

Employees are responsible for handling information according to its classification.

7. Access Control and Identity Management

Access to OHI Group systems and information must be:

- Authorised
- Appropriate to job responsibilities
- Regularly reviewed

OHI Group applies the principle of:

"Least privilege access"

meaning users receive only the access necessary to perform their role.

Employees must:
- Protect passwords and credentials
- Never share accounts
- Report suspicious access activity
- Lock devices when unattended

8. Cybersecurity and Technology Protection

OHI Group will maintain appropriate cybersecurity controls to protect technology environments.

Security measures may include:
- Endpoint protection
- Network security
- Vulnerability management
- Security monitoring
- Backup and recovery processes
- Encryption
- Multi-factor authentication
- Patch management

Employees must:
- Use approved systems and devices
- Avoid unauthorised software
- Report suspicious emails or activity
- Follow acceptable technology use requirements

9. Third-Party and Supplier Security

Third parties may create information security risks.

OHI Group will assess security requirements when engaging:
- Technology providers
- Cloud providers
- Consultants
- Contractors
- Suppliers with system access

Contracts should include appropriate requirements relating to:
- Data protection
- Confidentiality
- Security controls
- Incident reporting
- Compliance obligations

10. Cloud, Digital Transformation and AI Security

OHI Group recognises the importance of digital transformation and responsible adoption of emerging technologies.

Cloud services, digital platforms, and AI solutions must be implemented responsibly and securely.

Security considerations must include:
- Data protection
- Access controls
- Supplier security
- Regulatory compliance
- Responsible AI practices

Employees using AI tools must comply with OHI Group requirements regarding:
- Confidential information
- Personal data
- Intellectual property
- Accuracy and verification of outputs

11. Information Security Awareness and Responsibilities

Cybersecurity is everyone's responsibility.

Employees must:
- Complete required security awareness training
- Understand their security responsibilities
- Protect company information
- Report incidents and concerns

Managers must ensure their teams understand applicable security requirements.

12. Information Security Incident Management

OHI Group maintains processes to identify, report, investigate, and respond to security incidents.

Examples include:
- Data breaches
- Lost devices

- Malware incidents
- Unauthorised access
- Information leakage
- Cyber attacks

Employees must immediately report suspected incidents.

Early reporting helps reduce impact and supports effective response.

13. Business Continuity and Resilience

OHI Group will maintain appropriate measures to ensure critical systems and information remain available during disruptions.

This includes:
- Backup processes
- Recovery planning
- Resilience measures
- Crisis response arrangements

14. Governance and Accountability

Board of Directors
Provides oversight of information security risks and organisational resilience.

CEO and Executive Leadership Team
Responsible for ensuring cybersecurity receives appropriate strategic attention and resources.

IT and Information Security Function
Responsible for:
- Security strategy
- Cybersecurity controls
- Monitoring
- Risk management
- Awareness programmes

Business Leaders
Responsible for ensuring information security requirements are implemented within their areas.

Employees
Responsible for protecting information and complying with this Policy.

15. Monitoring, Assurance and Review

OHI Group will monitor effectiveness through:
- Security assessments
- Internal audits
- Vulnerability reviews
- Compliance monitoring
- Incident analysis
- Training completion reviews

This Policy will be reviewed every two years or earlier where significant changes occur.

Failure to comply with this Policy may result in disciplinary action, including termination of employment or contractual relationships.