Compliance Policy

Confidential

Document Control

Document Name	Compliance Policy		
Version No.	1.0	Document No.	POL/2022/07
Creation Date	25-Nov-2016	Release Date	10-Oct-2017
Classification	Internal	Effective Date	10-Oct-2017
Prepared By	Information Security Team	Document Owner	CISO
Reviewed By	Rajan Merwade	Approved by	Anil Nimbargi

Document Version History

Version No.	Effective Date	Revision Description	Approved By
1.0	10-Oct-2017	Creation	Anil Nimbargi
1.1	30-Apr-2020	Distribution List	Rahul Shandilya
1.2	01-Jun-2022	Overall revision and review	Anil Nimbargi
1.3	16-Jan-2024	1. Updated Welspun Group and Companies to Welspun World 2. Overall review and revision	Anil Nimbargi

Distribution

Sr. No.	Distribution List	Type of Access
1	ISO/CISO/GCTO	Full Access
2	Welspun Employees	Read Only

Table of Contents

1. Purpose

The purpose of this policy is to ensure compliance of the information systems to the organizational security policies, avoid breaches of any statutory, regulatory or contractual obligations of any information security requirements and to maximize the effectiveness of the system audit process.

2. Scope and Applicability

This policy applies to Welspun World (hereafter referred to as 'Welspun') IT environment information assets covered within the Information Security Management System ('ISMS') scope.

3. Policy statement

3.1 Applicable legislation and contractual requirements

- All relevant statutory, regulatory and contractual requirements shall be explicitly defined and documented for all information systems.
- Specific controls and individual responsibilities to meet these requirements shall be defined and documented.
- Country specific compliance requirements shall be identified by appointed representatives from relevant departments.

3.2 Intellectual property rights

- Appropriate procedures shall be implemented to ensure compliance with legal restrictions on the use of material which are protected by intellectual property rights.
- Maintaining awareness of policies to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them.
- Maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.
- Implementing controls to ensure that any maximum number of users permitted within the license is not exceeded.
- Not duplicating, copying or converting to another format or extracting from commercial recordings (film, audio, books, articles & reports) other than permitted by copyright law.

3.3 Software compliance

- All required software licenses shall be purchased from reputable sources and inventory of all software installed on computers shall be maintained and regularly checked for compliance.
- Only authorized personnel shall have access to original copy of the software media, license and manuals and they shall be preserved.
- Backup copy of any media, if made, shall comply with the license agreement and the numbers of backup copies are restricted to the agreed upon quantity in the license agreement.
- Users shall not be allowed to install any software on their computers.

- Regular checks shall be carried out to ensure that authorized software and licensed products are installed.
- Any freeware if required by user; shall be approved by the IT team for business purposes before installation. License and support agreement of the same shall be downloaded and preserved.

3.4 Protection of records

- Important records shall be identified to meet statutory or regulatory requirements, as well as to support essential business activities.
- Evidence shall be identified to prove security incidents or frauds and securely preserved.
- Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements.
- Media, holding the records, shall be securely stored in a fireproof cabinet or similar secured storage.
- Media shall be tested regularly to prevent loss of any records stored on media due to degradation of media with time.
- Data storage system shall be chosen such that required data can be retrieved in a manner acceptable to a court of law, in acceptable timeframe and acceptable format.
- An inventory of critical information required by the organization shall be maintained.
- Guidelines shall be issued on the retention, storage, handling and disposal of records and information
- A retention schedule shall be drawn up identifying records and the period of time for which they shall be retained

3.5 Privacy and protection of Personally Identifiable Information

- Company shall collect required personal data from employees, temporary workers/contractors, and its customers.
- Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
- Personal data of all employees, third party vendors, customers and temporary workers/contractors shall be used only for the purpose for which it was collected. It shall not be shared with anyone on request or for any reasons except for a need to know and approved by the respective authority or the owner.

3.6 Regulation of cryptographic controls

- Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.
- Restrictions on import or export of computer hardware and software for performing cryptographic functions shall be considered.
- Legal advice shall be sought to ensure compliance with relevant legislation and regulations for cryptographic controls.

3.7 Compliance with security policies and standards

- Every employee shall ensure that information security policies comply within their area of responsibility.
- Review shall be conducted against the information security policies on a periodic basis.
- Asset owners of information systems shall support regular review of the compliance of their systems with the appropriate security policy, standards and other security requirements. They shall also act upon the findings of such reviews and implement suggestions.

3.8 Technical compliance review

- Technical compliance review shall be performed annually for all critical information systems to ensure that hardware and software controls have been correctly implemented.
- Penetration testing and vulnerability assessment shall be performed on all critical systems at least once in a year to identify vulnerabilities on the systems.
- Penetration testing and vulnerability assessment could lead to compromise of the security of the system and inadvertently exploit other vulnerabilities. Such test shall only be carried out by, or under the supervision of competent, authorized persons.

3.9 Independent review of the information security

- The Information Security Management Forum (ISMF) shall initiate an independent review of Information Security Management System (ISMS).
- The review shall include assessing opportunities for improvement and need for changes to approach to security, including policies and procedures.
- Reviews shall be carried out by individuals independent of the area under review and with appropriate skills and experience.
- The results of the independent review shall be recorded and reported to the ISMF.
- If the independent review identifies that the organization's approach and implementation to managing information security is inadequate, e.g., documented objectives and requirements are not met or not compliant with the direction for information security stated in the information security policies, management shall consider corrective actions.

4. Consequence Management

Any violation to this procedure should be handled as per consequence management procedure. Refer:

Welspun-Consequence management procedure.

5. Exception

Any deviation to this policy shall be handled as per exception handling procedure Refer: Welspun-ISMS-Exception handling procedure.