

<b>Doc. No. : WIL/SCS/01</b>	<b>Welspun Living Limited</b>	<b>Supply Chain Security – Policies &amp; Procedures Manual</b>
<b>Section No. : 06</b>	<b>Section Title: SOP –CYBER SECURITY</b>	

**OBJECTIVES:**

The factory protects its IT system from illegal use and access through the use of firewalls, employee passwords, and anti-virus software. Login / password are required to access the IT system which is confidential. The most common threat to organizations comes from viruses, worms, and other hostile programming code. The company ensures the protection of its IT security through various measures including educating users to the threats, setting out policies that minimize the infection potential, installing antivirus software, regularly updating the antivirus software, and installing all of the security patches for operating systems, web browsers, email clients, and applications.

The main purpose is to inform company users: employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the company. The Cyber Security Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

**POLICY STATEMENT:**

The company is committed to adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorized employees, and to ensure the integrity of all data and configuration controls. This policy will deal with the following domains of security:



- Computer system security: CPU, Peripherals, OS. This includes data security.
- Physical security: The premises occupied by the IT personnel and equipment.
- Operational security: Environment control, power equipment, operation activities.
- Procedural security by IT, vendor, management, personnel, as well as ordinary users.
- Communications security: Communications equipment, personnel, transmission paths, and adjacent areas.

**A. THREATS TO SECURITY**

**1. Employees**

One of the biggest security threats is employees. They may do damage to your systems either through incompetence or on purpose. You have to layer your security to compensate for that as well. You mitigate this by doing the following.

- ✓ Only give out appropriate rights to systems. Limit access to only business hours.
- ✓ Don't share accounts to access systems. Never share your login information with co-workers.
- ✓ When employees are separated or disciplined, you remove or limit access to systems.
- ✓ Advanced – Keep detailed system logs on all computer activity.
- ✓ Physically secure computer assets, so that only staff with appropriate need can access.

<b>Prepared &amp; Reviewed by : RK Choudhary</b> 		<b>Approved by : Director &amp; Business Head</b> 
<b>Issue No. : 07</b>	<b>Revision No. : 06</b>	<b>Date of Review:- March 15, 2024</b>

<b>Doc. No. : WIL/SCS/01</b>	<b>Welspun Living Limited</b>	<b>Supply Chain Security – Policies &amp; Procedures Manual</b>
<b>Section No. : 06</b>	<b>Section Title: SOP –CYBER SECURITY</b>	

## 2. Amateur Hackers and Vandals.

These people are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. These are usually crimes of opportunity. These amateur hackers are scanning the Internet and looking for well known security holes that have not been plugged. Web servers and electronic mail are their favorite targets. Once they find a weakness they will exploit it to plant viruses, Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness they are likely to move on to an easier target.

## 3. Criminal Hackers and Saboteurs.

The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network

## **B. WHAT ARE WE PROTECTING**



It is the obligation of all users of the company systems to protect the technology and information assets of the company. This information must be protected from unauthorized access, theft and destruction. The technology and information assets of the company are made up of the following components:

- Computer hardware, CPU, disc, Email, web, application servers, PC systems, application software, system software, etc.
- System Software including: operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
- Application Software: used by the various departments within the company. This includes custom written software applications, and commercial off the shelf software packages.

Communications Network hardware and software including: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

## **C. PROCEDURES:**



1. The Company protects its IT system from illegal use by providing employee passwords and by using anti-virus software. Trend-Micro anti-virus software is used for protection of data, and the system is updated automatically on daily basis. All the systems are provided with anti-virus software to secure data.
2. Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore they are prohibited from

<b>Prepared &amp; Reviewed by : RK Choudhary</b> 		<b>Approved by : Director &amp; Business Head</b> 
<b>Issue No. : 07</b>	<b>Revision No. : 06</b>	<b>Date of Review:- March 15, 2024</b>

<b>Doc. No. : WIL/SCS/01</b>	<b>Welspun Living Limited</b>	<b>Supply Chain Security – Policies &amp; Procedures Manual</b>
<b>Section No. : 06</b>	<b>Section Title: SOP –CYBER SECURITY</b>	

making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of the company.

3. Daily, weekly and monthly backup of applications' data is performed using the back-up solutions. so that the data shall be preserved even if the main IT system is disabled in the case of virus attack, fire at the factory etc.
4. E- Mail facility to required stations within the factory through Microsoft Office solutions i.e. Office 365.
5. Whole system is connected through LAN (Local Area Connection), in order to facilitate the exchange of information between the key users and the internet connectivity is provided by dedicated ILL service by Tata communications.
6. All employees having access to the computer system are changing their passwords periodically – generally once in 45 days for security reasons and the Passwords are generally be a combination of letters, symbols and numbers, about minimum of 6 mixed characters in length. The IT system is locked immediately after 3 unsuccessful attempts of login. In case if a user login the system and could not able to login even after 3 attempts, the user shall be locked out of the system automatically, and he/she should contact the IT administrator. Invalid password attempts are automatically recorded, and the IT Head conducts review on invalid password attempts.
7. If an employee suspects that another person may have discovered the password, the password shall be immediately changed. In addition, there is a process to disable the system access of the employee who have left or terminated or resigned the employment.
8. Only the authorized employees are having access to IT system, so that the computer network is secure. Any form of abuse of IT system such as improper access, tampering or the altering of business data etc, shall be subject to investigation/ enquiry and serious disciplinary action in accordance with the provisions of the certified standing order.
9. Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to company systems for which they do not have authorization.
10. Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the designated approvers.
11. Users shall not download unauthorized software from the Internet onto their PCs or workstations. Users are required to report any weaknesses in the company computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

<b>Prepared &amp; Reviewed by : RK Choudhary</b> 		<b>Approved by : Director &amp; Business Head</b> 
<b>Issue No. : 07</b>	<b>Revision No. : 06</b>	<b>Date of Review:- March 15, 2024</b>



<b>Doc. No. : WIL/SCS/01</b>	<b>Welspun Living Limited</b>	<b>Supply Chain Security – Policies &amp; Procedures Manual</b>
<b>Section No. : 06</b>	<b>Section Title: SOP –CYBER SECURITY</b>	

12. For IT disaster Management, all the business critical applications are hosted in cloud based tier-IV primary data center at Mumbai with DR site at Hyderabad. The Organization has Network Administrator and other employees in IT who are there to lead the IT disaster recovery team.
13. The computer server rooms are defined as high security rooms and are restricted to the access of authorized persons only.
14. The IT review meeting shall be conducted once in every month. The IT head is vested with the responsibility to review the IT issues/problems and call for the meeting for necessary action.
15. Cyber security threats and unauthorized attempts shall be reported to IT Head, and if necessary, it shall also be reported to local law enforcement and business partners including contractors, Suppliers and customers.

#### **D. USER CLASSIFICATION**

All users are expected to have knowledge of these security policies and are required to report violations to the Security Administrator. The company has established the following user groups and defined the access privileges and responsibilities:

<b>User Category</b>	<b>Privileges &amp; Responsibilities</b>
Department Users (Employees)	Access to application and databases as required for job function.
System Administrators	Access to computer systems, routers, hubs, and other infrastructure technology required for job function. Access to confidential information on a “need to know” basis only.
Security Administrator	Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function.
Systems Analyst/Programmer	Access to applications and databases as required for specific job function. Not authorized to access routers, firewalls, or other network devices.
Contractors/Consultants	Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function. Knowledge of security policies. Access to company information and systems must be approved in writing by the company director.
Other Agencies and Business Partners	Access allowed to selected applications only when contract or inter-agency access agreement is in place or required by applicable laws.

<b>Prepared &amp; Reviewed by : RK Choudhary</b> 		<b>Approved by : Director &amp; Business Head</b> 
<b>Issue No. : 07</b>	<b>Revision No. : 06</b>	<b>Date of Review:- March 15, 2024</b>

<b>Doc. No. : WIL/SCS/01</b>	<b>Welspun Living Limited</b>	<b>Supply Chain Security – Policies &amp; Procedures Manual</b>
<b>Section No. : 06</b>	<b>Section Title: SOP –CYBER SECURITY</b>	

General Public	Access is limited to applications running on public Web servers. The general public will not be allowed to access confidential information.
----------------	---------------------------------------------------------------------------------------------------------------------------------------------

**E. MONITORING USE OF COMPUTER SYSTEMS**

The company has the right and capability to monitor electronic information created and/or communicated by persons using company computer systems and networks, including e-mail messages and usage of the Internet. It is not the company policy or intent to continuously monitor all computer usage by employees or other users of the company computer systems and network. However, users of the systems should be aware that the company may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with company policy.

**F. USER SYSTEM AND NETWORK ACCESS – NORMAL USER IDENTIFICATION**

All users will be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with management & supervisory personnel and/or any other employee whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:



1. Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
2. Password must be changed every (45 days).
3. User accounts will be frozen after (3 attempts) failed logon attempts.
4. Logon IDs and passwords will be suspended after 90 days without use.

Users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this document.

Employee Logon IDs and passwords is deactivated as soon as possible if the employee is terminated, fired, suspended, or otherwise leaves the employment of the company office.

Supervisors / Managers shall immediately and directly contact the company IT Manager to report change in employee status that requires terminating or modifying employee logon access privileges.

Employees who forget their password must raise the ticket to IT department to get a new password assigned to their account. The employee must identify himself/herself by (e.g. employee number) to the IT department.

<b>Prepared &amp; Reviewed by : RK Choudhary</b> 		<b>Approved by : Director &amp; Business Head</b> 
<b>Issue No. : 07</b>	<b>Revision No. : 06</b>	<b>Date of Review:- March 15, 2024</b>

<b>Doc. No. : WIL/SCS/01</b>	<b>Welspun Living Limited</b>	<b>Supply Chain Security – Policies &amp; Procedures Manual</b>
<b>Section No. : 06</b>	<b>Section Title: SOP –CYBER SECURITY</b>	

Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee’s password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

**G. SYSTEM ADMINISTRATOR ACCESS**

System Administrators, network administrators, and security administrators will have (type of access) access to host systems, routers, switches, and firewalls as required to fulfill the duties of their job.

All system administrator passwords will be **DELETED** immediately after any employee who has access to such passwords is terminated, resigned or otherwise leaves the employment of the company.

**H. CONNECTING DEVICES TO THE NETWORK**

Only authorized devices may be connected to the company network(s). Authorized devices include PCs and workstations owned by company that comply with the configuration guidelines of the company. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach to the network: non-company computers that are not authorized, owned and/or controlled by company. Users are specifically prohibited from attaching any external device/unauthorized media to the company network.



**NOTE:** Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. thumb drives and writable CD’s.

**I. REMOTE ACCESS**

Only authorized persons may remotely access the company network. Remote access is provided to those employees, contractors and business partners of the company that have a legitimate business need to exchange information, copy files or programs, or access computer applications. The only acceptable method of remotely connecting into the internal network is using a secure VPN access.

**J. UNAUTHORIZED REMOTE ACCESS**

The attachment of (e.g. hubs) to a user’s PC or workstation that is connected to the company LAN is not allowed without the written permission of the company. Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

<b>Prepared &amp; Reviewed by :</b> RK Choudhary 		<b>Approved by :</b> Director & Business Head 
<b>Issue No. :</b> 07	<b>Revision No. :</b> 06	<b>Date of Review:-</b> March 15, 2024

<b>Doc. No. : WIL/SCS/01</b>	<b>Welspun Living Limited</b>	<b>Supply Chain Security – Policies &amp; Procedures Manual</b>
<b>Section No. : 06</b>	<b>Section Title: SOP –CYBER SECURITY</b>	

**K. PENALTY FOR SECURITY VIOLATION**

The company takes the issue of security seriously. Those people who use the technology and information resources of company must be aware that they can be disciplined if they violate this policy. Upon violation of this policy, an employee of company may be subject to discipline up to and including discharge. The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state and national laws and all other relevant information. Discipline which may be taken against an employee shall be administrated in accordance with disciplinary action policy or certified standing order of the company.

In a case where the accused person is not an employee of company the matter shall be submitted to the local law enforcement. The Company may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

**L. SECURITY INCIDENT HANDLING PROCEDURES**



This section provides some policy guidelines and procedures for handling security incidents. The term “security incident” is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the company network. Some examples of security incidents are:

1. Illegal access of a company computer system. For example, a hacker logs onto a production server and copies the password file.
2. Damage to a company computer system or network caused by illegal access. Releasing a virus or worm would be an example.
3. Denial of service attack against a company web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
4. Malicious use of system resources to launch an attack against other computer outside of the company network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees, who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to the IT Head immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

**J. DISPOSAL:**

Hard disk and other media are crushed / drilled through / to destroy them and disposed of through authorized recycle vendor. These procedure are done under live video recording which are archived. A certificate is also issued by the recycler.

<b>Prepared &amp; Reviewed by : RK Choudhary</b> 		<b>Approved by : Director &amp; Business Head</b> 
<b>Issue No. : 07</b>	<b>Revision No. : 06</b>	<b>Date of Review:- March 15, 2024</b>