**JTL Defence Limited**
**Registered Office:** 1/10-B, First Floor,
Munshi Niketan Building, Asaf Ali Road,
New Delhi – 110002
**W:** www.rciind.com **E:** compliance@rciind.com
**M:** +919056585489
**CIN:** L24320DL1992PLC047055

# CYBER SECURITY AND DATA PRIVACY POLICY

## PURPOSE

The purpose of this document is to enable the IT security operations center team, incident handlers and responders with sufficient information and guidelines to follow when a cybersecurity crisis / incident occurs at JTL Defence Limited (Erstwhile RCI Industries & Technologies Limited).

This document aims at providing detailed information on the steps and the workflow to be followed in the event a cyber-security crisis incident occurs and to provide a frame work for managing and mitigating cyber security risks, to safeguard information from unauthorized access, protection of individual's personal information and to establish guidelines and procedures for safeguarding an organization's / individual's data and system.

The purpose of this policy is as below:

- This policy serves as a guide to ensure the confidentiality, integrity and availability of Company's information systems.
- To ensure the proper and lawful use of the Company's Information Technology system.

## POLICY STATEMENT(S)

JTL Defence Limited is committed to safeguard the Confidentiality, Integrity and Availability of all physical and electronic information of the organization to ensure that regulatory, operational and contractual requirements are fulfilled.

## SCOPE

The document applies to all the information technology, equipment and devices that are part of Company's cyber space environment such as desktops, laptops, applications, servers, databases, network devices, security devices equipment's etc.

This policy further applies to all Company's employees, suppliers, vendors consultants and/or individuals with access to Company's electronic system, information and/or hardware. The cyber security policy is published to all people who are the employees of the organization, suppliers, customers, shareholders and anyone who has temporary / permanent access to our systems.

## Company Policy

**JTL Defence Limited**
**Registered Office:** 1/10-B, First Floor,
Munshi Niketan Building, Asaf Ali Road,
New Delhi – 110002
**W:** www.rciind.com **E:** compliance@rciind.com
**M:** +919056585489
**CIN:** L24320DL1992PLC047055

## a) PROTECTION TO IT DEVICES OF THE COMPANY

- Protect the devices of the Company with strong credentials.
- Timely upgradation of the Anti-virus software.
- Only Company's technological assets are permitted to connect to the network of the Company.
- Sharing of company's network with the external agency is done under supervision and with due verification and approval.
- Enable dual authentication & alert when there is an attempt to access servers.

## b) PROTECTION TO INTERNAL, VENDOR AND CUSTOMER DATA

- Protection of all the data of the Company by giving the authorization and access to the right and desirable person.
- Access to all the data by logging in through the valid and secured credentials.
- Backing-up of data on a periodical basis.
- Categorization of the risk on the basis of its severity and taking necessary steps for its mitigation accordingly.
- Enable dual-factor verification and automatic alert notification pops up whenever someone attempts to access the server.

## c) HUMAN RESOURCE SECURITY

- Screening or background checks must be performed at time of hire.
- Employees shall sign the organization's terms and conditions of employment that includes the employee's and the organization's responsibilities for information security, at the time of hire.
- Employees must take Information security and Data Privacy training at the time of hire and annually thereafter, or as per the business needs.

## d) ASSET MANAGEMENT

- Company's information assets must be appropriately protected from theft, loss or any unauthorized access. Assets may include but not limited to:

– Documented business processes and activities (electronic or physical)
– Electronic information (data, spreadsheets, presentations, documents, notes, email, social media, etc.)
– Physical information (papers, signs, posters, etc.)
– Hardware (servers, laptops, desktops, printers, photocopiers, routers, switches, firewalls, mobile phones, tablets, computing devices, etc.)
– Software (databases, applications, utilities, productivity software, cloud services, etc.)

**JTL Defence Limited**
**Registered Office:** 1/10-B, First Floor,
Munshi Niketan Building, Asaf Ali Road,
New Delhi – 110002
**W:** www.rciind.com **E:** compliance@rciind.com
**M:** +919056585489
**CIN:** L24320DL1992PLC047055

- Network (communication links, wired network, wireless network, etc.)
- People (employees, contractors, interns, etc., as defined in this policy)
- Facilities (offices, data centers, server rooms, wiring closets, storage facilities, studios, etc.)

- An accurate and up-to-date inventory of critical assets must be maintained. Critical assets are those, which if compromised or lost, could cause significant business disruption or revenue loss. An asset owner must be designated for each inventoried critical asset, though assets remain JTL Defence Limited property.

## e) USER ACCESS MANAGEMENT

- Access to Company's information, information systems (Infrastructure, applications, source code repositories) and information processing facilities shall be controlled to prevent unauthorized access.
- Access shall be granted considering least privilege principle and on need-to-know basis only.
- Logs should be maintained for access granted to critical systems.
- All access to the servers and managed services is private, unless proxied through a public secure resource.
- Internal vulnerability assessment is performed at regular intervals.

## f) PHYSICAL AND ENVIRONMENTAL SECURITY

- Physical and environmental security requirements must be considered during design, buildouts or improvements of existing Company's facilities to protect against natural disasters, unauthorized access, malicious attacks and accidents.
- Access to Company's facilities must be restricted to authorized people only.
- Security barriers must be deployed at Company's facilities to protect the physical security perimeter consisting of walls, fences, doors, ceilings, floors, etc., to prevent unauthorized access, damage and interference.
- Where applicable or determined by business requirements, photo identification badges must be issued. People must wear or display badges when asked to do so.
- Visitors must be granted access to Company's facilities for business reasons only. Records of visitors access to Company's facilities must be maintained. As appropriate, visitors must be escorted within Company's facilities by a Company's person and display temporary identification, if issued during their visit.
- The delivery and loading areas must be monitored for unauthorized access and incoming and outgoing materials must be registered.
- Safeguards must be applied and regularly tested to prevent or mitigate damage to Company's facilities from fire, flood, earthquake, lightning and other natural and manmade disasters.
- Information processing facilities must be monitored for environmental conditions including temperature and humidity.

**JTL Defence Limited**
**Registered Office:** 1/10-B, First Floor,
Munshi Niketan Building, Asaf Ali Road,
New Delhi – 110002
**W:** www.rciind.com **E:** compliance@rciind.com
**M:** +919056585489
**CIN:** L24320DL1992PLC047055

- Power and telecommunications cabling carrying data or supporting information services must be protected from interception, interference and damage, wherever possible.

## g) EQUIPMENT SECURITY

- Equipment must be protected to minimize potential risks such as theft, fire, explosives, smoke, water, dust, vibration, electrical supply interference, electromagnetic radiation, vandalism and unauthorized access.
- Equipment must be protected from power failures and other disruptions caused by failures in electricity, telecommunications, ventilation, air conditioning, etc.
- Equipment supporting the business processes must be maintained and tested regularly according to manufacturer recommended service intervals. Maintenance records must be maintained.
- Equipment, except assigned portable/mobile devices such as laptops, mobile phones and tablets, must not be taken off site without approval. Records of incoming and outgoing equipment must be maintained and reviewed periodically.
- Appropriate protection must be applied to protect laptops, mobile phones, tablets, etc., while working remotely from home or other offsite locations.

## h) APPLICATION SECURITY

- Application security testing shall be performed at regular intervals to find and fix any issues/vulnerabilities.
- Changes to applications shall be performed through defined processes and requisite approvals to ensure security during change management activities.
- Only approved, tested and authorized changes shall be made to the applications.
- Changes shall be reviewed periodically by the respective Product manager/Engineering Manager to ascertain whether appropriate change management processes were followed or not.

## i) VENDOR SECURITY MANAGEMENT

- Vendor's access to Company's information/information assets shall be restricted.
- Ensure a vendor risk assessment is performed to validate the adequate security controls of the vendor having access to Company's critical data.
- Where third parties are involved in processing of Personal Data it must be ensured that due diligence is performed with respect to data security and privacy. It must also be ensured that data privacy obligations that are applicable to JTL Defence are transferred to the third parties

## j) POLICY ON DATA PRIVACY

- Well-established roles and responsibilities.

**JTL Defence Limited**
**Registered Office:** 1/10-B, First Floor,
Munshi Niketan Building, Asaf Ali Road,
New Delhi – 110002
**W:** www.rciind.com **E:** compliance@rciind.com
**M:** +919056585489
**CIN:** L24320DL1992PLC047055

- Establish data retention and safe disposal using archiving tools.
- Annual review of records to ensure that updates to the data processing activities are reflected accurately.
- Practice shall be made where personal data should not be processed manually and for the access of the same, an approval from the requisite authority should be required.

## k) EXCEPTIONS

Where there is a justifiable business need that requires actions to be performed which are in conflict to this document, such exceptions shall be reported to the IT Head and CFO and approval shall be obtained. Such approvals shall be valid for a pre-defined period after which it shall be re-evaluated and re-approved.

**********