

# **Policy Framework on Cyber Security, Data Privacy and Business**

## **Continuity**

### **I. Introduction And Objective**

In today's world, Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. Due to prevailing digitalization in all walks of life, there has been an exponential increase in online transactions. Secured cyberspace is both a national and global challenge due to an exponential increase in online transactions environment. Ensuring the Confidentiality, Integrity, and Availability (CIA triad) of information is the fundamental goal of information security and cybersecurity. As a result, RITES has formulated this policy to help outline the security measures put in place to ensure information remains secure and protected.

### **II. Policy Guidelines**

1. It is pertinent that all adopt and imbibe a culture of cyber security in day-to-day working to keep personal and organizational data safe through better cyber hygiene.
2. As a measure of Cyber Security implementation, company shall implement:-
  - Firewall which protects our applications and data from cyber threats.
  - Anti-virus software at end points and gateway level to counter any attack from viruses.
  - Password protection so that no unauthorized person can access our network/system.
  - Secured & protected email for correspondence

All devices, desktop/laptops etc shall be registered for allowing the network access to these devices.

3. The company shall establish and ensure continuous monitoring of Network Security Management, Network Access Control, User Registration and De-registration, Facility Management, Perimeter Security, Risk Assessment and Treatment, Information Continuity, Cyber Security Incident Management, Data Center Operations and Disaster Recovery, Internet and Electronic Messaging, Maintenance of computers and peripherals etc.
4. For undisruptive work, the Company shall ensure server availability, application uptime, restoration of Datacentre, internet uptime, website availability uptime, email services uptime, backup schedule, etc.

### **III. Framework**

For handling various functions / processes, Company shall ensure implementation and compliance of Information Security Management System (ISMS) standard including standard as specified by ISO 27001:2013.

### **IV. Data Privacy**

Data privacy is associated with the proper handling of personal and business data and also extends to other valuable or confidential data of the organization. The importance of data privacy is directly related to the business value of data. It shall be entrusted to keep data confidential and secure by exercising sound data management and preventing unauthorized access that might result in data loss, alteration or theft. The company shall implement the necessary Data Privacy controls. Confidentiality and non-disclosure clauses shall be incorporated into RITES contracts with its business partners.

### **V. Business Continuity and Disaster Management Plan**

For Business Continuity and Disaster Management following shall be ensured:-

- Disaster Recovery site shall be maintained.
- DR drills shall be conducted on regular intervals.
- Implementation of Business Continuity and Disaster Management Plan ('Plan") shall be ensured. The brief framework of the plan is as under :

- The Business Continuity and Disaster Management Plan in RITES Ltd. offices is a comprehensive framework designed to mitigate and effectively respond to various emergencies and disasters that may occur within the premises. The plan aims to safeguard the lives of employees, protect company assets and ensure the business continuity in the face of adverse situations.
  - The plan begins with thorough risk assessment to identify potential hazards such as fires, natural disasters, chemical spills, medical emergencies or security breaches. Based on the evaluation, the plan outlines specific response protocols and assigns responsibilities to designated personnel.
  - The plan includes clear evacuation procedures, including designated assembly points and escape routes along with the establishment of emergency response team responsible for coordinating evacuation efforts and providing necessary assistance to employees. Regular drills and training sessions are conducted to ensure that employees are well prepared to respond appropriately during emergencies.
  - In addition to above, the plan addresses communication strategies during disasters, ensuring that emergency notifications and alerts reach all employees promptly. It also establishes channels for effective communication with external agency associated with emergency services and relevant stakeholders.
  - Overall, disaster management plan in RITES Ltd. office is a proactive and well-structured approach to emergency preparedness, response and recovery aimed at ensuring the safety of employees and minimizing the impact of disasters in the organization's operations.
- Continuous performance monitoring shall be done to ensure business continuity and further improvement.