भारत पर्यटन विकास निगम लि.
India Tourism Development Corporation Ltd.
(भारत सरकार का उपक्रम)
(A Government of India Undertaking)

Ref : IT/HQ/CSP/2023

Cyber Security Policy

India Tourism Development Corporation Limited
Registered Office: Scope Complex, Core – 8
7, Lodhi Road
New Delhi - 110003

भारत पर्यटन विकास निगम लि.
India Tourism Development Corporation Ltd.
(भारत सरकार का उपक्रम)
(A Government of India Undertaking)

Cyber Security Policy

ITDC Cyber Security Objectives

ITDC shall enable cyber security framework consisting of structured and well-defined policies, procedures and guidelines while addressing the following objectives:

• Critical information, data and assets are protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional by implementing technical, process, people control.

• To run computers and applications virus free and recovering from cyber security incidents pertaining to phishing attack.

• Awareness programs on information/ cyber-security are imparted to all employees and wherever applicable to third parties.

• Ensuring continual improvement to the ITDC cyber security posture.

The Cyber security defends computers, servers, mobile devices, networks, and data from malicious attacks. The cyber threat could be from anywhere so different rules /paths are used for defending the all these areas to make safe the Data/Servers/Computers/Notebooks.

1. ITDC shall ensure Network security through Unified Threat Management System for security policies, standards, for security procedures validated and audit program. It is used for securing a computer network from intruders, whether targeted attackers or opportunistic malware. It is operationalised through NIST Cybersecurity Framework and ISO 27001 controls. Sophos includes firewalls, malware detection, and Managed Detection and Response service that monitor the environment 24/7. The following are the security controls of the unified threat management system **Data protection, privacy, and security.**

   - **Risk management**
   - **Access and user management**
   - **Password management and authentication controls**
   - **Firewall protection**
   - **Encryption and key management**
   - **Threat and vulnerability management**
   - **Secure development life cycle and bug bounty program**
   - **Threat modelling**
   - **Network security – zero-trust network model**
   - **Physical security**

2. **ITDC shall ensure Application security through Firewall protection that helps screen out hackers and worms that try to reach to end user over the Internet. All messages entering or leaving the Internet pass through the firewall present and Antivirus installed to keep device safe, secure, protects against malicious virus attacks at end user.**
3. **ITDC shall ensure Information security through Firewall protection, Threat modelling, both in storage and in transit. It protects the integrity and privacy of data. The Antivirus installed at end user protects from local vulnerabilities through which the Network securities keeps safe Data mitigates the effects of cyber-attacks against the system.**
4. **ITDC shall ensure Operational security through securing Data. The Data is secured and safe while the processes and handling data assets. The permissions users have when accessing a network through Access and user management and the end user Antivirus protects while sharing mode.**
5. **ITDC shall ensure End-to-end user security through end user Antivirus procedure making safe with virus attacks, USB drives infections and unauthorized users.**
6. **ITDC shall ensure Cloud security through enhancing the security, Security Information Management and Security Event Management functions are combined in to one Security Management System. Web application firewall protects the web applications by filtering and monitoring http traffic between a web application and internet. DDoS (Distributed Denial of Service attack) protection keeps services available in case of a Volumetric DDoS attack.**
7. **ITDC shall ensure e-Mail security through providing the two-factor authentication to the user for accessing their government email service.**

    a. **Password authentication**
    b. **OTP authentication**

Review and Compliance

Responsibility for compliance with the Policies lies with Head-IT and nominated representatives. The Policy will be reviewed once annually.