# CYBER SECURITY POLICY



## HINDUSTAN AERONAUTICS LIMITED

15/1, CUBBON ROAD, PB.NO 5150

BENGALURU – 560 001

# Cyber Security Policy

## I. Introduction:

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited. The growth and penetration of IT systems has exposed them to varied threats emanating from internal and external sources. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secured cyber space. HAL has adopted Cyber Security Policy as detailed below as an umbrella framework for defining and guiding the initiatives and reactive measures towards secured cyberspace.

## II. Vision

To build a secure and resilient cyberspace for HAL, its customers and all stake holders.

## III. Mission

To provide highest level of IT service across HAL, positioning Cyber Security, Data protection and privacy as a key enabler.

This document belongs to Hindustan Aeronautics Limited, 15/1, Cubbon Road, P.B.No. 5150, Bengaluru – 560 001
Any unauthorized distribution in hardcopy or softcopy or any other media is strictly prohibited.

## IV. Objectives

1) To create a secure cyber ecosystem, generate adequate trust and confidence in the IT systems and transactions carried out in the cyberspace, and thereby achieving adoption of IT in all business process.

2) To create an assured framework for design of security policies, enabling compliance to global security standards, and deploying best practices identified through conformity assessment (product, process, technology and people).

3) To develop/ deploy suitable security technologies towards achieving Secured ICT Assets meeting HAL's overall security requirements.

4) To enable protection of information while in process, handling, storage and transit so as to safeguard privacy of personal and sensitive data and avoiding economic losses primarily due to cybercrime or data theft.

5) To encourage the culture of alert and responsible behavior towards cyber security from all users through continual and effective communication

## V. Strategies

### A. Creating a Secure Cyber Ecosystem

1) Designate a Cyber Security Organization Structure under CISO to coordinate all matters related to cyber security in HAL, with clearly defined roles and responsibilities for all stakeholders in Offices/ Divisions.

2) Develop relevant information security policies duly integrated with their business plans and implement such policies aligning with the best practices. These policies may include advisories received from various agencies like CERT-In, Cyber Security Group (MoD), Cyber Information Research Agency towards compliance requirements.

This document belongs to Hindustan Aeronautics Limited, 15/1, Cubbon Road, P.B.No. 5150, Bengaluru – 560 001
Any unauthorized distribution in hardcopy or softcopy or any other media is strictly prohibited.

3) Allocate specific Capital and Revenue Budgets towards implementing cyber security initiatives and meeting emergency response arising out of cyber incidents.

4) Encourage stakeholders to install, upgrade and strengthen information infrastructure towards bettered prepared cyber security posture.

5) Ensure data privacy by strictly limiting data access on need to know basis. Keep the personally identifiable information (PII) e.g. Aadhaar Number, PAN Number, Bank Account Number, Passport Number etc. is stored with adequate security measures and access restrictions.

**B. Creating an Assured Framework**

1) Adopt global best practices to the maximum extent feasible in information security and compliance and thereby enhancing cyber security posture.

2) Create infrastructure complying with conformity assessment and requirements as mandated by various adopted International Standards, Internal System Audits, Vulnerability Assessment and Penetration Testing (VAPT) by CERT-In Empanelled Auditors etc.

3) Enable implementation of global security best practices in the formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all concerned.

4) Identify and classify information infrastructure facilities and assets at entity level considering risk perception for undertaking commensurate security protection measures, such as separation of private and public networks etc.

5) Encourage secure application/ software development processes complying with the known best practices.

This document belongs to Hindustan Aeronautics Limited, 15/1, Cubbon Road, P.B.No. 5150, Bengaluru – 560 001
Any unauthorized distribution in hardcopy or softcopy or any other media is strictly prohibited.

6) Create conformity assessment framework for periodic verification of compliance to standard, guidelines, audit observations and other adopted benchmarks on cyber security.

7) Encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and accordingly take steps for periodic patching/ upgrade.

**C. Strengthening the Compliance Framework**

1) Mandate periodic audit and evaluation of adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to CSG (DDP/MoD) Guidelines.

2) Enable, educate and facilitate awareness of the Cyber Security Guidelines.

3) Ensuring appropriate physical, logical, and procedural controls are in place to preserve confidentiality, integrity, availability and privacy of information.

**D. Creating mechanisms for security threat early warning, vulnerability management and response to security threats**

1) Create systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions.

2) Cooperate and coordinate with National Level Computer Emergency Response Team (CERT-In) in dealing with National Cyber Crisis Situations.

This document belongs to Hindustan Aeronautics Limited, 15/1, Cubbon Road, P.B.No. 5150, Bengaluru – 560 001
Any unauthorized distribution in hardcopy or softcopy or any other media is strictly prohibited.

3) Implement Cyber Crisis Management Plan towards dealing with cyber incidents adversely impacting critical processes or endangering safety and security

4) Conduct and facilitate regular cyber security drills/ audits/ exercises to enable assessment of the security posture and level of preparedness in resisting and dealing with cyber security incidents.

5) Adopt advanced techniques and solutions towards enhancement in degree of data protection.

## E. Sensitization of Human Resource on Cyber Security

1) Mandate cyber security training infrastructure through Computer Based Training

2) Facilitate cyber security training for Cyber Security Professionals.

3) Maintain records of general awareness assessment, professional training on cyber security and knowledge base adequacy assessment on Cyber Security

## F. Creating Cyber Security Awareness

1) Promote a comprehensive companywide awareness program on security of cyberspace through continual and effective communication (e.g. Newsletters).

2) Sustain security awareness and publicity campaign through electronic media such as companywide screensavers.

3) Conduct, support and enable cyber security workshops / seminars and certifications.

This document belongs to Hindustan Aeronautics Limited, 15/1, Cubbon Road, P.B.No. 5150, Bengaluru – 560 001
Any unauthorized distribution in hardcopy or softcopy or any other media is strictly prohibited.