


<b>Amber Enterprises India Limited</b>	 <b>AMBER GROUP</b>	<b>CYBER SECURITY POLICY</b>
<b>CSP/2023/08</b>		<b>Date of Issue: 16 May 2023</b>

# The Amber Group


## CYBER SECURITY POLICY

<b>Document Name</b>	<i>Amber Group Cyber Security Policy – A subset of Amber IT Policy</i>
<b>Preface</b>	Modern companies and businesses have become increasingly dependent on technology for collection, storage, retrieval and general management of huge amount of data and information. Security breaches to such technology can adversely affect business operations, with potentially far-reaching financial implications, and damage to company reputation. Appropriate measures are required to be put in place to safeguard the systems against human errors, hacker attacks, and system malfunctions.
<b>Release Date</b>	16 May 2023
<b>Issued By</b>	Business Responsibility and Sustainability Committee
<b>Approved By</b>	Board of Directors ('BoD')

### 1. DEFINITIONS

<b>Term</b>	<b>Definitions</b>
Amber	Amber Enterprises India Limited
Associates	It includes directors, KMPs, employees, agents, representatives, vendors, contractors and business partners or any other persons/individuals, who may be acting on behalf of the Company.
Group Companies	It means all the Subsidiary(ies), Step-down Subsidiary(ies) and Associate(s) companies of Amber.
Cyber security	Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

**Amber Enterprises India Limited**  
**CIN : L28910PB1990PLC010265**  
**Corporate Office:** Universal Trade Tower, 1<sup>st</sup> Floor, Sector -49, Sohna Road, Gurgaon -122 018  
**Regd. Office:** C-1, Phase – II, Focal Point, Rajpura Town – 140 401, Punjab  
**Phone – 0124 3923000 Fax – 0124 -3923016, Website – [www.ambergrouppindia.com](http://www.ambergrouppindia.com),**  
**Email Id – [infoamber@ambergrouppindia.com](mailto:infoamber@ambergrouppindia.com)**

<b>Amber Enterprises India Limited</b>	 <b>amber</b> <b>AMBER GROUP</b>	<b>CYBER SECURITY POLICY</b>
<b>CSP/2023/08</b>		<b>Date of Issue: 16 May 2023</b>

## 2. OBJECTIVE

This cyber security policy is a set of guidelines spelling out acceptable practices and procedures that minimize the vulnerability of company data, networks and infrastructures to accidental or malicious attacks. This policy sets out to do this by giving guidelines on how to preserve the integrity of our data and technology infrastructure. The policy also spells out how to mitigate security risks


## 3. SCOPE

The policy applies to employees including virtual employees, contractors, value chain partners, any other person with partial or full access to our systems and information infrastructures.

## 4. CONFIDENTIAL DATA

All our employees are required to preserve the sanctity of confidential information and data which includes, but not limited to:


- Financial reports that are not published.
- Information about our clients, business partners, and vendors.
- Patents, formulas or new technologies.
- Personnel secrets, including salaries and terms of service.
- Contact details of our existing and prospective customers
- Documents and details of company assets like land, buildings, and vehicles.

<b>Amber Enterprises India Limited</b>	 <b>amber</b> <b>AMBER GROUP</b>	<b>CYBER SECURITY POLICY</b>
<b>CSP/2023/08</b>		<b>Date of Issue: 16 May 2023</b>

## 5. POLICY STATEMENT

- We are committed to protect Company and Personal Devices by doing the following
  - ✓ Keeping all devices' passwords protected.
  - ✓ Not leaving the devices unattended or exposed.
  - ✓ Ensuring modern antivirus software in the devices.
  - ✓ Updating security software of the browsers and systems as soon as the updates are available.
  - ✓ Ensuring only secure networks to log into company accounts and systems.
  - ✓ Preventing other peoples' devices to access our internal systems
  - ✓ New employees being issued with company devices will be required to keep them safe by following laid down instructions
  
- We ensure the safe operation of Emails by following steps:-
  - ✓ Being careful of clickbait titles with fascinating information or rewards.
  - ✓ Avoiding opening attachments or links whose content is invitingly vague
  - ✓ Being careful of inconsistent and poorly formatted emails that smack of unprofessional sources
  - ✓ Checking email sources
  
- We are committed to ensure the sanctity of Passwords by doing the following: -
  - ✓ Avoiding use of inferential passwords that can easily be guessed from one's antecedents, like birthdays, names of children, etc.
  - ✓ Choosing passwords with at least eight characters in a hard-to-guess pattern, like interspersing capital with lower-case letters, numbers, and symbols.
  - ✓ Changing passwords at regular intervals.
  - ✓ Exchange of credentials to be done by phone instead of email.
  - ✓ A password management system /tool to be installed that can generate and store passwords

**Amber Enterprises India Limited**  
**CIN : L28910PB1990PLC010265**  
**Corporate Office:** Universal Trade Tower, 1<sup>st</sup> Floor, Sector -49, Sohna Road, Gurgaon -122 018  
**Regd. Office:** C-1, Phase – II, Focal Point, Rajpura Town – 140 401, Punjab  
**Phone – 0124 3923000 Fax – 0124 -3923016, Website – [www.ambergroupindia.com](http://www.ambergroupindia.com),**  
**Email Id–[infoamber@ambergroupindia.com](mailto:infoamber@ambergroupindia.com)**

<b>Amber Enterprises India Limited</b>	 <b>AMBER GROUP</b>	<b>CYBER SECURITY POLICY</b>
<b>CSP/2023/08</b>		<b>Date of Issue: 16 May 2023</b>

- We ensure the security of Data in Transit by undertaking the following steps: -
  - ✓ Sensitive data should be transferred only when there is a genuine need for the same
  - ✓ Confidential data to be shared over the company network
  - ✓ Recipients of the data must be properly authorized
  - ✓ Prompt reporting of any hacking attempts, privacy breaches or related scams to the head of IT.
  
- We take extra measures to ensure cyber security by following steps: -
  - ✓ Reporting any stolen or damaged equipment as soon as possible
  - ✓ To turn off their screens when leaving the desks
  - ✓ Change all passwords immediately when a device is lost.
  - ✓ Steer clear of suspicious websites.
  - ✓ Not to download suspicious, unauthorized and illegal software on the company devices.
  - ✓ Investigating security breaches and advising the company accordingly.
  - ✓ Install firewalls, anti-malware software, and access authentication systems.

## 6. REVIEW OF POLICY

The Business Responsibility and Sustainability Committee shall review and amend the policy from time to time as and when deemed fit and make recommendations on any changes required to the Board for consideration and approval.

*‘Commitment is Key to Cybersecurity Success’*

**Amber Enterprises India Limited**  
 CIN : L28910PB1990PLC010265  
**Corporate Office:** Universal Trade Tower, 1<sup>st</sup> Floor, Sector -49, Sohna Road, Gurgaon -122 018  
**Regd. Office:** C-1, Phase – II, Focal Point, Rajpura Town – 140 401, Punjab  
**Phone –** 0124 3923000 **Fax –** 0124 -3923016, **Website –** www.ambergroupindia.com,  
**Email Id–**[infoamber@ambergroupindia.com](mailto:infoamber@ambergroupindia.com)