Oriental Aromatics

Cyber Security & Data Privacy Policy

Cyber Security and Data Privacy Policy

1. Objectives

Oriental Aromatics Limited (OAL) recognizes the significance of protecting information in all forms and the crucial role that information technology plays in the company's operations. OAL feels the need to make more of an effort to protect the information and the technology resources that support it as more information is used and shared digitally by authorized users of OAL's IT resources. As a result, OAL has developed this Policy. Privacy and usage guidelines for OAL's Information Technology Resources are also addressed in the Policy.

Our guidelines and provisions for maintaining the security of our data and technology infrastructure are outlined in our company's cyber security policy.

We become more susceptible to serious security breaches as we increase our reliance on technology for information collection, storage, and management. Our company's reputation could be jeopardized and significant financial damage could be caused by human errors, hacker attacks, and system failures. We have taken a number of security measures as a result. Additionally, we have prepared instructions that may assist in mitigating security threats.

This policy aims to ensure that all users use the OAL Information and Information Systems lawfully, ethically, and professionally to advance the OAL's interests.

2. Scope and Applicability

This policy applies to everyone who, in India, has access to OAL's Information Technology Resources and it shall be the responsibility of all Factory Managers at respective factories and IT Head at the corporate office to ensure that this policy is clearly communicated, understood and followed by all users.

This Policy also applies to all contracted staff and vendors/suppliers providing services to OAL that bring them into contact with OAL's Information Technology resources. The HR / Admin department and the respective Factory Managers who contracts for these services shall be responsible to provide the contractor/vendor/supplier with a copy of this Policy before any access is given to them.

This policy covers the usage of all of the company's information technology and communication resources, whether they are owned or leased by the company or are under the company's possession, custody, or control, including but not limited to:

2.1. All computer-related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, PDAs, wireless computing devices, telecom equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected.

2.2. All electronic communications equipment, including telephones, pagers, radio communicators, voicemail, e-mail, fax machines, PDAs, wired or wireless communications devices and services, Internet and intranet and other on-line services.

2.3. All software including purchased or licensed business software applications, OAL -written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on OAL -owned equipment.

2.4. All intellectual property and other data stored on OAL's Information Technology equipment.

2.5. These policies also apply to all users, whether on Company property or otherwise, connected from remote connections via any networked connection, or using Company equipment.

2.6. Usage of Oriental Aromatics website: http://www.orientalaromatics.com/

3. Definitions

a. Information Technology Resources: Information Technology Resources for purposes of this Policy include, but are not limited to, OAL owned or those used under license or contract or those devices not owned by OAL but intentionally connected to OAL - owned Information Technology Resources such as computer hardware, printers, fax machines, voice-mail, software, e-mail and Internet and intranet access.

b. User: Anyone who has access to OAL's Information Technology Resources, including but not limited to, all employees, temporary employees, probationers, contractors, vendors and suppliers.

c. Sensitive Personal Data: Sensitive Personal Data of a person, under the Indian Information Technology Rules 2011, means such Personal Data which consists of information relating to:

- Password
- Financial Information such as bank account or credit card or debit card or other payment instrument details
- Physical, physiological and mental health condition
- Medical records and history
- Biometric Information
- Sexual orientation
- Any other details relating to the above mentioned, provided by any person to OAL for providing services

4. Policy

a. Cyber Security:

Confidential data is secret and valuable. Unpublished financial information, Data of customers/partners/vendors, Patents, formulas or new technologies, Customer lists (existing and prospective) are common confidentiality data at OAL. This policy will provide our employees a guideline to avoid security breaches.

b. Personal and company devices protection:

Employees introduce a security risk to our data when they use their digital devices to access company accounts or emails. We advise our employees to secure both their personal computers, tablets, and mobile phones as well as those that the company provides. This is possible if they:

- Secure all devices with a password.

- Select and upgrade a comprehensive antivirus program.
- Ensure that they never leave their devices unattended or exposed.
- Install browser and system security updates every month or as soon as they become available.
- Use only private, secure networks to access company accounts and systems.

Additionally, we advise our employees not to borrow other people's devices or access internal systems and accounts from them.

c. Keep emails safe:

Emails sometimes host malicious software (like worms.) and scams. To avoid the scams and virus infections, we instruct employees to:

- Not to open attachments or click on links, when the content is not adequately explained
- Be doubtful to clickbait titles
- Verify the legitimacy of any messages they receive by checking the email addresses and names of the recipients.
- Look for inconsistencies or giveaways.

If an employee is unsure on the safety of the email they received, they can refer to the IT Head or IT Team.

d. Password management

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret.

For this reason, we advise our employees to:

- Have passwords with at least eight characters, including all-caps and lower-case letters, numbers, and symbols, and they should not include information that is simple to guess.
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every two months.

e. Transfer data securely

Data transfer poses a security risk. Employees must:

- Unless absolutely necessary, avoid transferring sensitive data to other devices or accounts (such as employee records, information about suppliers or customers, etc.). We advise employees to seek assistance from our IT helpdesk whenever massive transfers of such data are required.
- Use the company network or system to share confidential information, not a private connection or public Wi-Fi.

- Ensure that the person or organizations receiving the data have the appropriate authorization and adhere to adequate security policies.
- Scams, privacy breaches, and hacking attempts must be reported to our IT team so that they can better safeguard our infrastructure. For this reason, we encourage our employees to promptly notify our IT Team for any suspected attacks, suspicious emails, or phishing attempts. When necessary, our IT team will conduct an immediate investigation, resolve the issue, and issue a company-wide alert.

We also instruct our employees to take the following additional precautions to lessen the likelihood of security breaches:

- Turn off their screens and lock their devices when leaving their desks.
- Contact the HR or IT department as soon as possible if any equipment is lost or damaged.
- When a device is stolen, all account passwords must be changed at once.
- Report the company of a potential security flaw or perceived threat.
- Avoid installing suspicious, illegal, or unauthorized software on their company equipment.
- Avoid visiting suspicious websites.
- We also expect our employees to comply with our Information Technology Policy.

Our IT Team had:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.
- Our company will have all physical and digital shields to protect information.

f. Remote employees

This policy's instructions must also be followed by remote employees. They are required to adhere to all data encryption, protection standards, and settings because they will be accessing our company's accounts and systems from a distance. Additionally, they must ensure that their private network is secure.

g. Take security seriously.

Everyone, covering all the stakeholders, should have confidence in the security of their data and feel that their data is safe at OAL. The only way to earn their trust is to actively safeguard our databases and systems. We can all contribute to this by being vigilant and keeping cyber security top of mind.

h. Privacy Policy

OAL believes that Companies which fail to protect personal data and comply with data privacy regulations aren’t just risking financial penalties. They also risk operational inefficiencies, intervention by regulators and most importantly permanent loss of consumer

trust. This Policy is applicable to all data collected, received, possessed, owned, controlled, stored, dealt with or handled by OAL in respect of a stakeholders.

i. Information we collect.

For the purpose of providing the stakeholders with efficient service, we may collect sensitive information that is absolutely needed, from these sources:

- Our website: We may collect information about data entered on our website, resources accessed on the webpage and transactions carried through our websites.
- Subscription: All information that are fed by stakeholders to receive our newsletters or updates will be stored with us.
- Correspondence: Any correspondence received with our marketing representatives, procurement personnel, associates, employees, consultants, sales affiliates, distributors, agents, etc. may be stored by us.
- Vendor or Supplier data collected during commercial transactions through Purchase, Sales, Sale Orders, Purchase Orders, Vendor/Customer registration and other means.
- Other sources: Any information we get from sources that aren't related to or about our business, like public information from social networks, market research, and other sources can be gathered. The Internet protocol (IP) address used to connect a user computer or device to the Internet, the browser type and version, time zone setting, browser plug-in types and versions, operating system and platform, and anonymous data collected by the hosting server for statistical purposes may also be stored by us.

j. Storage of Data

All collected data is kept safe in our databases or in the databases of our service providers, protected by reasonable organizational, technical, and security measures. To make it easier to safely transfer the data to our service providers or another organization when necessary, we ensure that the data is encrypted in accordance with our security policy.

OAL will keep the data for as long as it takes to accomplish the goals for which it was collected. We never keep the data for longer than is absolutely necessary.

h. Usage and disclosure of data collected

We use all data in a way that is legal, fair, and open in order to serve our legitimate business interests. The Data may be used for the following purposes:

- for marketing and internal administration purposes;
- managing our relationships with prospects and customers by processing orders and responding to requests;
- for demographic characterizations and internal marketing surveys in aggregate;
- to facilitate contract performance or performance;
- to generate data analytics that will enhance our web user experience, services, and communication quality; and for any other specific purpose that was specified when the information was collected.

OAL reserves the right, notwithstanding anything contained herein, to transmit Data to other interested parties when:

- we have consent to share the data;
- we need to share the information to provide the product or service;
- we need to send the information to businesses that provide products or services on behalf of OAL;
- we respond to court orders or legal process;
- we need to protect and defend the rights or property of OAL or enforce any terms and conditions for use and transactions; or
- we find that some actions which violates any of our policies / procedures.

i. Policy for Website usage

Any personal information shared in our Website shall be kept confidential. Personal information, shared on our website is used for doing the intended business. By visiting our website, the visitors thereby grant their consent to OAL Limited to store and use such information.

OAL reserves its rights to collect, analyse and disseminate aggregate site usage patterns of all its visitors with a view to enhance its services to the visitors. This includes sharing the information within OAL and business associates as a general business practice.

In the course of its business, OAL may hold on-line contests and surveys as permitted by law and it reserves its right to use and disseminate the information so collected to enhance its services to the visitors.

Cookies: - To personalize visitors experience on OAL's Website or to support one of its promotions, OAL may assign visitor computer browser a unique random number (cookie). "Cookies" enhance website performance in important ways like personalizing experience, or making the visitor's visit more convenient. Privacy and security will not be compromised when the visitor accept a "cookie" from OAL Limited's Website.

In case the visitor do not wish to receive cookies, they may do so my modifying thier browser preferences.

5. Disciplinary Actions

OAL may consider any violation of this policy to be misconduct. Any infractions of this code of conduct will result in disciplinary action. These actions will vary based on the nature of the violation. All of the below mentioned disciplinary measures are up to management discretion and may not be taken in the order listed. Concerning the appropriateness of the disciplinary action for the violation, Human Resources shall be consulted.

Individual or collective violations of this policy may result in disciplinary measures such as the following, but are not limited to:

- Counselling;
- A warning in writing or verbally;
- Complete or partial removal of system privileges and access; and
- Any combination of the preceding.

Disciplinary measures may include, but are not limited to, the following in the event of a serious or persistent violation of this policy:

- Demotion
- Termination or Suspension
- Loss of benefits for a specific period of time or indefinitely
- Any combination of the above
- Taking legal action

6. Cyber Security and Data Privacy Governance

Cyber Security and Data Privacy Governance Structure consists of the IT Head, Site IT Head and System Admins.

IT Head shall also be part of the overall Cyber Security and Data Privacy Governance Structure.

These personnel are responsible for development, implementation, operation, maintenance and continual improvement of Cyber Security and Data Privacy at OAL.

7. Raise your concern

Grievance Officer

In accordance with the Information Technology Act, 2000 and the rules framed thereunder, the name and contact details of the Grievance Officer are provided below:

IT Head,

Oriental Aromatics Limited,

Jehangir Building,

133, Mahatma Gandhi Road,

Kala Ghoda, Fort,

Mumbai, Maharashtra 400001

+9122 6655 6000

9AM - 5PM (on all working days)

Please get in touch with a member of OAL's IT team if you have any inquiries regarding this policy.

Please get in touch with OAL's Compliance team at cs@orientalaromatics.com if you think someone may have violated this policy.

Retaliation, reprosal, or subsequent discrimination against anyone who raises a concern or reports possible misconduct is strictly prohibited at OAL.

In accordance with its internal procedures for investigations, OAL will conduct an investigation into alleged misconduct relating to this Policy. Any OAL employees who

violated this policy may face disciplinary action, including termination from their employment.