Information Security Policy

Version 9.1

May 2022

Table of Contents

Title	Information Security Policy
Owner	Grasim IT
Prepared By	Grasim IT
Reviewed By	
Approved By	
Approval Status	
Classification	General
Distribution List	All

Document Revision and Change Control

Sr. No.	Version	Date	Changes
1.	1	1st Oct, 2007	Document Created
2.	2	1st Dec, 2009	Amended the policy to merge Information Systems AUP and Internet and Email AUP. Other wording changes.
3.	3	12th Jul, 2010	Amended the policy to add Confidential and Personal data protection clause
4.	4	25th Mar, 2021	Amended the policy on acceptable usage, disciplinary actions and other important aspects as per ISMS
5.	5		Amended the policy to add Remote Work Security clause. Amended and made necessary updates to statements 4.1.1, 4.1.7, 4.2.5, 4.4.4, 4.5.1,4.5.2, 4.6.2, 4.8.2, 4.8.5 4.14.10, and 4.13.2 Added statements 4.4.7, 4.7.4, 4.7.5, 4.8.7, 4.9.5, 4.10.5, 4.12.6, 4.13.4 and 4.14.9

Confidentiality Statement

This page has been intentionally left blank.

1 Objective

This policy is a Directive, which is binding for the entire GIL and comes into effect upon adoption and publication by the respective company management.

The purpose of this policy is to ensure that all users use the GIL Information and Information Systems in a professional, ethical, and lawful manner in furtherance of the interests of the GIL.

2 Applicability

This document outlines policies for acceptable use of Grasim's Information and Information Systems (defined hereinafter).

It also applies to the handling of all the personal data of natural persons, in particular, the data of customers, shareholders, employees and other third parties, contracting parties or business partners

3 Definitions

For the purpose of this policy,

1. "Grasim Industries Limited" collectively refers to all the legal entities belonging to the Grasim Conglomerate and as further stated on its website https://www.grasim.com.
2. "Company" or "Unit" refers individually to each legal entity within GIL.
3. "Grasim's Information Systems" include any application, computer, server, electronic media, communication devices network, Information Technology services, its websites (including cloud, internet, intranet & email) provided. Supported, procured, leased, or used by GIL and containing any Grasim's Information. The policy set forth herein also shall apply to any service or device (including personal computing devices such as smart phones, tablets etc.) owned or procured by the user and used for accessing GIL Information and Information Systems.
4. "Grasim's Information" includes any kind of information or data (including internet, email, SMS, instant messaging, etc.), whether tangible or intangible, contained in or stored on Grasim's Information Systems.
5. A "user" of the Grasim's Information System is any Person (including employees, trainees, contractors, and third parties) who has been provided access to Grasim's Information Systems.
   A "Person" for the purpose of this policy shall include an individual, corporation, limited liability company, partnership, association, joint venture, trust, unincorporated organization, or other entity not part of the GIL, including any governmental entity.
6. An "asset" is any data, device, or other component of the environment that supports information related activities.

4 Policy Statements

4.1 Acceptable use of assets

4.1.1 Grasim's Information Systems are to be used only for processing data and information relating to the GIL's businesses and obtained through legal means. Any use of the Grasim's Information and Information Systems for any direct or indirect personal illicit gain is strictly prohibited.

4.1.2 The Grasim routinely monitors usage patterns for its e-mail/Internet communications and other IT services and systems. All messages created, stored, sent, or retrieved over the Grasim's Information Systems are the property of the GIL and shall not be considered private information. The GIL reserves the right to access and monitor all electronic messages, and soft or hard copy files of the user's communications at all times in accordance with the relevant laws of the country.

4.1.3 Users shall not attempt to access any data or programs contained on the Grasim's Information Systems for which they do not have authorization or explicit consent of the data owner.

4.1.4 Users shall not use the GIL Information Systems in a manner that would violate any applicable law, regulation or any GIL policies or procedures.

4.1.5 Users shall not use Grasim's Information Systems to store any un-published, confidential, or price-sensitive information belonging to a Person outside the GIL unless such usage or storage has been duly approved by the owner of such information. A user shall be personally liable for any unauthorized use or storage of such third-party information.

4.1.6 Users shall not use the Grasim's Information Systems for any activity that will be:

a) discriminating, harassing, vilifying or victimizing others based on gender, race, religious beliefs, disability, political conviction, sexual preferences, age, or otherwise;

b) degrading the performance of the Grasim's Information Systems;

c) gaining access to any Grasim's Information System for which proper authorization has not been given;

d) depriving an authorized user access to an authorized Grasim's Information System;

e) attempting to gain more system access or privileges than authorized;

f) circumventing the security measures governing the Grasim's Information or the Grasim's Information Systems;

g) sharing information with a Person outside the GIL, which will allow the circumvention of the Grasim's security systems or the infiltration of the Grasim's Information Systems by such third party; and

h) causing physical or other damage to the Grasim's Information Systems or property.

i) unlawful, fraudulent, threatening, libellous, defamatory, obscene or otherwise objectionable, or infringing or violating any party's intellectual property rights.

4.1.7 Use of any communication facilities not provided or authorized by the GIL for any official communication is prohibited. Users shall not use any unauthorized / personal e-mail services (e.g. Gmail, outlook.com, yahoo, etc.), instant messengers (e.g. Google chat, WhatsApp, Telegram, Facebook chat, etc), or communication facilities for the transmission, storage, or retrieval of Grasim's Information.

4.2 Data Classification and sharing

4.2.1 Based on the data classification norms adopted by relevant Company or Unit from time to time, users shall classify information based on its nature, value, criticality, sensitivity, and legal requirements, and considering the impact to the GIL if such information were disclosed to a third party, altered, or destroyed without authorization. All users must handle the Grasim's Information strictly as per its classification.

4.2.2 Users shall not, without the prior consent of the Company, divulge the Company's confidential information, whether electronic, oral, or written, to any third party or for any purpose other than the benefit of the Company and GIL.

4.2.3 Messages or information sent by a user to a Person outside the GIL via any Grasim's Information System (including any communication utilizing or travelling over an electronic network owned or leased by the GIL), constitute statements that reflect on GIL. Therefore, all such communication should be done in a manner that is respects the Grasim's security and image.

4.2.4 Users will be held responsible and liable for any defamatory, obscene, offensive, political, proprietary, copyrighted, or libellous content they may post, propagate, transmit, or store using the Grasim's Information Systems or any personal computing devices, email, social media, or blog sites. Third parties may pursue legal action against individuals personally for the content uploaded onto such social media platforms.

4.2.5 Users must not make multiple copies of confidential documents in paper or electronic form unless it is deemed required by the competent authority.

4.2.6 Users shall not leave confidential documents in publicly accessible areas such as conference rooms, around printers, open desk areas etc.

4.2.7 Users shall destroy unwanted copies of confidential documents using a paper shredder before disposing them of.

4.3 General Obligation

4.3.1 Users shall familiarize themselves with the contents of the latest Grasim's information security policy and Seamex HR SSC Information Security Policy, which is available on Grasim website (and any updates to these) and adhere to the same.

4.3.2 Users shall comply with Grasim's security directives, guidelines, and polices at all times. Users shall not circumvent or attempt to circumvent any logical or physical security controls or guidelines issued by GIL or the Company. Additionally, users shall proactively participate in all security and safety exercises, drills, and training that may be conducted from time to time by the GIL or the Company.

4.3.3 If a user becomes aware of any weaknesses in the security of the Grasim's Information Systems or of any incidents of possible misuse or violation of this policy, such user shall report the same to her/his manager or CISO.

4.3.4 Users must ensure that devices (e.g., desktops, laptops, tablets, phones, etc.) used for accessing GIL Information or in furtherance of the business of the Company or Unit are duly secured, sanitized and supervised by relevant Company or Unit and are used in compliance with the latest Grasim's information security policy and Seamex HR SSC Information Security Policy

4.3.5 Users are responsible for protecting Grasim's Information in their possession including information stored on the Grasim's Information Systems to which such users have access. Additionally, users are obligated to abide by the lawful policies and procedures of all networks and systems with which they communicate, technically support, and/ or utilize.

4.4 Passwords

4.4.1 Users will be fully accountable for their passwords and any access related to these passwords

4.4.2 Users must ensure to change their default/first time password given to them by IT helpdesk at the first login.

4.4.3 Users will set strong passwords having at least 8 characters in length, consisting a mixture of alphabets, both upper and lower cases, numbers, and special characters. Passwords must not contain all or a recognizable part of the user name

4.4.4 Passwords must be changed every 90 days or as and when there is a need. Users should not repeat their previous five passwords or passwords used during the last 12 months.

4.4.5 Users must never share their passwords with anyone including the IT helpdesk personnel and administrators.

4.4.6 Users must input all passwords themselves, when receiving technical assistance instead of sharing the passwords with the helpdesk. Users must not write down or store passwords in readable format.

4.4.7 Users must not use the "Remember Password" feature of applications.

4.5 Data Backup

4.5.1 Users shall take regular backups of the business data residing in their workstations. Additionally, users must prioritize the backup of critical and sensitive data, and if deemed necessary, ensure a more frequent backup interval. The backup shall be taken only on assets which are owned by the organisation

4.5.2 Users shall not share/store any business information on their personal devices (e.g. Pen Drive, Hard disk, mobile phone, etc.) or email IDs (e.g. Gmail, outlook.com, Hotmail, etc.)

4.6 Laptop Security

4.6.1 Users shall never leave laptops unattended for extended periods of time. If required to be left in the office, user shall make sure that it is locked and stored in a secure area at the end of the workday.

4.6.2 Users shall ensure that the laptop/desktop has the company provided antivirus program/endpoint security solution installed and configured for automatic updates

4.6.3 Users shall ensure that all removable storage media such as USB drives, and CDs are scanned before use.

4.6.4 Users shall take due care to protect their laptop devices and the official data stored therein from loss, theft and misuse. Loss/theft of such devices should be immediately notified to the respective Managers, Chief Information Security Officer (CISO), and/or the Chief Information Officer (CIO) of their respective Company or Unit, so that official data stored therein is prevented from any misuse.

4.7 Software Use

4.7.1 Users shall not download or install any unauthorized software onto any Grasim's Information System where by any Grasim's Information is stored.

4.7.2 Users shall not make copies of copyrighted software, unless permitted by the copyright owner. As used herein, "copyright owner" refers to the Person which possesses the exclusive right to make copies, license, and otherwise exploit a literary, business, musical, or artistic work, whether printed, audio, video, etc.

4.7.3 At all times, users are responsible for the content that they download, store, post, or transmit using GIL Information Systems, including mobile computing devices. Subject to allowable exemptions, copyrighted materials belonging to any Person outside the GIL shall not be, transmitted by employees on GIL Information Systems. All users obtaining access to third party information or materials must respect all copyrights and shall not copy, retrieve, modify, or forward copyrighted materials, except with written permission of the copyright owner, or as may be permitted by applicable law. Each user shall observe all terms and conditions of the applicable license agreement under which a license to use any copyrighted work has been obtained.

4.7.4 Users must only use the software for purposes defined, and only on GIL Information Systems covered, by the agreement, contract, or license.

4.7.5 Users must not upload any GIL data / information on any free online software, converters or file sharing websites (e.g. PDF converter, WeTransfer, etc). Such act must not be done for any official purpose. Only applications approved / provisioned by IT team shall be used.

4.8 Social Engineering

4.8.1 When asked for confidential data including personal information, users should first check the identification of the individual before sharing any data.

4.8.2 Users must not divulge confidential GIL information over the phone or via SMS or emails without verifying the identity of the caller or sender first.

4.8.3 Users must not be pressurized or manipulated into giving out information.

4.8.4 Users must not reveal sensitive information on voicemail or on answering machines.

4.8.5 Users must watch out for 'shoulder surfers' or people who read confidential information on computer screens. Users should avoid entering credentials in the nearby presence of others.

4.8.6 Users must report any inappropriate request for company information from anybody to respective managers. In addition, users must seek the advice of respective managers before sharing confidential information with anyone.

4.8.7 Users should not download any files before validating the authenticity of the sender and his/her purpose.

4.9 Mobile computing

4.9.1 Only users enrolled in the Company's Mobile Device Management program may use personal mobile devices to process GIL information.

4.9.2 All personal devices shall use only licensed and authorized versions of operating system and applications. The use of customized, pirated, "rooted" or "jail broken" versions of the device is prohibited.

4.9.3 Users must not use external email accounts or file share utilities to synchronize Company's information to other personal devices or to cloud storage solutions.

4.9.4 Employees should be aware that, upon separation from the Company, IT function shall remove Company information from the user's mobile device.

4.9.5 Users should NOT download any organisation data / email attachments to any personal devices, including mobile phone. If file gets auto-downloaded for open/viewing purpose, it must be deleted in non-recoverable way, immediately after it is closed.

4.10 Physical Access

4.10.1 Users must always wear access card/ identification badge in the office premises

4.10.2 Users must enter and leave the office premises using their own access card and not use another individual's / colleague's card. Users shall never do tailgating nor encourage tailgating to enter the premise. (Tailgate is to closely follow an individual to enter premises without using an access card)

4.10.3 Users must not loan their access card to others

4.10.4 Users must keep the administration department informed in case of loss of the access card or identification badge.

4.10.5 Employees must escort visitors within the company premises.

4.11 Internet Security

4.11.1 Internet shall be used only for GIL businesses approved business purpose.

4.11.2 Internet medium shall not be used for purposes which are against GIL businesses rules and other legal regulations of the state.

4.11.3 Internet access shall not be used in any manner that would be discriminatory, harassing, or obscene, or for any other purpose that is illegal, against GIL businesses, or not in the best interest of GIL businesses.

4.11.4 Downloading of software, applications and other data is not permitted unless authorized and shall be as governed by the IPR and other license agreements.

4.11.5 Internet access by users using either GIL businesses owned devices or personal devices allowed access to GIL businesses networks shall be logged and monitored by the IT department to ensure compliance with Internet access policy.

4.11.6 Users shall not launch any social media handle, page using company name and logo without written permission of the authorized Corporate Communication Team personal.

4.12 Email Security

4.12.1 The personal/official devices used for email access (e.g. Desktops, laptops, tablets, phones) used must be authorized, secured and controlled by GIL. This policy shall also apply for personal devices used for official purposes. All other devices shall be prohibited from accessing GIL emails and information. Access to emails over the internet will be restricted to personal devices authorized, secured and controlled by GIL.

4.12.2 Users shall not use third party email systems (e.g. Google, Yahoo, Hotmail etc.) to store, transmit and/or process official information. Additionally, users shall be prohibited from copying/ forwarding official emails and information to such unauthorized third-party email systems.

4.12.3 The use of e-mail for transmission of chain/ hoax/ defamatory/ obscene/ offensive messages or information disparaging to others based on race, national origin, gender, sexual orientation, age, disability, religion, or political beliefs is not permitted under any circumstances.

4.12.4 The e-mail system shall not be used to solicit or advocate for commercial ventures, religious or political causes, outside GIL businesses, or other non-job-related solicitations.

4.12.5 The E-mail system shall not be used in violation of any or other person's rights. Disparaging or libellous comments shall not be made nor may any copyrighted material be used without proper authorization. Violations could result in liability for the individual as well as to the company.

4.12.6 Users should enable spam filters to ensure protection against potential malware and phishing.

4.13 Clean Desk and Clear Screen

4.13.1 Users shall ensure that their desk is kept clear of unnecessary paper documents during and after office hours. While leaving, users must ensure that all paper documents and files are locked away in cabinets.

4.13.2 Users shall ensure that all prints are immediately collected from the printer tray and fax machines.

4.13.3 Users shall make sure that their computer screen is locked while they are away from their computer

4.13.4 Sensitive information on paper that is to be shredded must not be left unattended to be handled later. They must be shredded immediately, or securely stored until the time that they can be shredded.

4.14 Privacy and personal data protection

4.14.1 Users shall treat the personal data of the Grasim employees, customers and business partners fairly and lawfully. Users entrusted with the task of collecting personal data shall do so only for specific, lawful, explicit, and legitimate purposes in furtherance of the Grasim's business. Further users shall process such data consistent with those purposes.

4.14.2 Users shall obtain and process only the data that is necessary and directly related to his/her duties; and will not collect excessive personal data than required

4.14.3 Users shall retain said data in such a way that outside third parties are prevented from becoming aware of it;

4.14.4 Users shall disclose and divulge data only with authorised personnel and in line with the procedures laid out by the organisation

4.14.5 Users shall ensure that said data is appropriately destroyed after the business purpose is served.

4.14.6 Users shall familiarize themselves with their data privacy obligations. Users can make use of available e-learning trainings to ensure the same.

4.14.7 Users shall protect personal data that is in his/her custody from unauthorized access

4.14.8 Users shall contact Data Protection Officer (in the following circumstances:

a) if there has been a Personal Data Breach
b) If there is a need to transfer personal data outside of the country
c) if you need any assistance dealing with any rights invoked by a Data Subject/principal
d) when engaging in a significant new, or change in, Processing activity involving personal data or plan to use Personal Data for purposes others than what it was collected for
e) While undertaking any activities involving Automated Processing including profiling or Automated Decision-Making
f) when carrying out direct marketing activities
g) while getting into contracts in relation to sharing Personal Data with third parties (including our vendors)

4.14.9 Users must never re-identify or attempt to re-identify anonymized personal data.

4.14.10 User must not use the GIL data or system for any illegal or unauthorized uses.

Examples of illegal or unauthorized uses include, but are not limited to: Modifying, adapting, translating, or reverse engineering any portion of the Grasim's Information Systems; using any robot, spider, site search/retrieval application, or other device to retrieve or index any portion of Grasim's Information Systems; collecting any information about other Members (including usernames and/or e-mail addresses) for

unauthorized and/or unlawful purposes; reformatting or framing any portion of the web pages or site images that are part of Grasim's Information Systems; creating user accounts by automated means or under false or fraudulent acts; creating or transmitting unwanted electronic communications such as "spam," or chain letters to other Members or otherwise interfering with other Member's enjoyment of the service; submitting materials of any third party without such third party's prior written consent; submitting materials that falsely express or imply that such materials are sponsored or endorsed by Grasim's Information Systems; submitting materials that infringe, misappropriate or violate the intellectual property, publicity, privacy or other proprietary rights of any party; transmitting any viruses, worms, defects, Trojan horses or other items of a destructive nature; submitting materials that are unlawful or promote or encourage illegal activity; displaying an advertisement as part of your profile; any automated use of the system, including the use of scripts to send messages or post comments; or submitting false or misleading information or any combination of these examples listed or any other act or omission similar to these examples.

4.15 Remote Work Security

4.15.1 Users must not connect to unsecure public Wi-Fi.

4.15.2 Users must ensure that they create a strong, unique password to connect to their home router. They should also change the SSID, enable the strongest network encryption protocol available, and limit access to specific MAC addresses.

4.15.3 Users should ensure that each videoconference meeting is private, either by requiring a password for entry or controlling guest access from a waiting room. While videoconferencing, users should blur their background to prevent others from spying on objects which may reveal sensitive data about themselves or GIL.

4.15.4 Users must be connected to Grasim's VPN at all times while accessing GIL Information Systems remotely.

4.15.5 Users shall equip a sliding webcam cover to enforce security and privacy.

4.15.6 Users must enable two-factor or multi-factor authentication where applicable.

4.15.7 Users must ensure that their devices are up-to-date on patches and compliant with Grasim's Information Security Policy.

5 Disciplinary Actions

GIL or the company may take any breach of this policy as a sign of misconduct by the user. The Disciplinary actions shall be taken as a consequence of any violations of this code of conduct. These actions will vary depending on violation committed. All the below mentioned disciplinary actions are subject to management discretion and will not necessarily follow the order in which they are listed. Human Resources shall be consulted regarding the appropriateness of the disciplinary action being applied for violation.

Disciplinary actions that may be taken as a consequence of violation of this policy, either by individuals or groups, include, but are not limited to:

a) Counselling;

b) Verbal or written warning;

c) Withdrawal of access and system privileges in part or whole; and

d) Any combination of above.

Serious or repeated breach of this policy can be construed as gross misconduct and disciplinary actions may include, but are not limited to:

a) Demotion;

b) Suspension or Termination;

c) Loss of benefits for a definite or indefinite time;

d) Any combination of the above.

e) Legal Action.