Information Systems Use Policy

Effective date: September 1, 2021

Available on the Avient Ethics & Corporate Policies Page on the Loop

Table of Contents

PURPOSE

This Information Systems Use Policy ("Policy") establishes acceptable and prohibited uses of Avient's Information Systems to protect Avient and its employees and affiliates from both intentionally and unintentionally harmful actions by Users.

SCOPE

This policy applies to all Avient Information Systems and all Users of Avient Information Systems, regardless of physical location, to the extent allowed by applicable law.

USAGE

Avient provides User access to Information Systems to facilitate business communications and advance Avient business objectives.

EXPECTATIONS FOR USE OF INFORMATION SYSTEMS

Users shall:

- Use all Information Systems consistent with their intended purpose, Avient business objectives, and the Code of Conduct;
- Take necessary steps to prevent unauthorized access to and maintain security of Confidential Data;
- Use only approved and secured methods when sharing Confidential Data and ensure recipients have authorization to receive Confidential Data and/or have obtained prior approval from User's manager; and
- Obtain approval from Avient's Information Technology department before procuring, installing, connecting, using, or decommissioning software, systems, applications, or non-Avient devices to or from Information Systems, including, but not limited to, on premise and cloud-based systems.

PROHIBITED USES OF INFORMATION SYSTEMS

Users shall not use Avient Information Systems for any of the following prohibited uses:

- Any activity prohibited by applicable law;
- Violating Avient Ethics and Corporate Policies;
- Infringing on the intellectual property rights of another individual or company;
- Soliciting for activities or products unrelated to Avient's business interests in furtherance of an independent business;
- Improper or unauthorized use of email and email distribution lists, including mass or unsolicited emails (such as chain letters) and forging email header information or signatures;
- Exporting, transferring, downloading, copying, or saving Confidential Data or Information Systems to non-approved devices or locations;
- Intentionally introducing security threats to Information Systems or effecting a Cyber or Data Incident; or
- Engaging in any other activity similar to the above that, in Avient's reasonable judgment, is disruptive to or not in the best interests of its business. This provision is not intended, and will not be used, to inhibit or chill employees' collective action rights or any other rights protected by law.

Additionally, the following Information Systems uses are prohibited unless specifically authorized by Avient or authorized Avient IT representatives:

- Revealing account usernames, passwords, or other Personal Data to others or allowing use of Information Systems by others, including family and other household members;
- Conducting any form of network monitoring that could intercept data not intended for the recipient User;
- Circumventing User authentication or security of any Information Systems; or
- Using personal devices to access Confidential Data or connect to Information Systems.

PERSONAL USE

Limited personal use of Avient Information Systems, including for social media and networking purposes, is acceptable, but must not breach any law or Avient policies, interfere with the User's or other employees' ability to fulfill employment obligations, negatively affect Information Systems, or otherwise violate this Policy.

Users shall store any personal files, notes, pictures, and emails in a separate and clearly identifiable folder labelled "PERSONAL EMAIL" or "PERSONAL FILES" such that Personal Data is always separate and readily distinguishable within Information Systems from Avient Data or otherwise Confidential Data.

SOCIAL MEDIA

Where Avient has created, operates, and/or sponsors a social media platform, only designated authorized Avient representatives may prepare or modify content for, present the views of, or speak on behalf of Avient.

Personal social media involving or referencing Avient must be in accordance with Avient Corporate and Ethics Policies.

ENFORCEMENT AND MONITORING

Authorized individuals within Avient IT may monitor or audit Information Systems use, whether company or personal, including, without limitation, Internet traffic and e-mail content, at any time and without prior notice to the User.

Users will immediately report violations of this Policy to the User's manager, an Avient Human Resources manager, or the IT Department. All Users must take reasonable action to avoid breaching this Policy.

Users have no right or expectation of privacy in Avient's Information Systems, to the extent allowed by applicable law. By using Avient's Information Systems, Users acknowledge the potential auditing, interception, or disclosure of data contained on or passing through Information Systems.

Employees found to have violated this policy will be subject to internal disciplinary action by Avient in appropriate cases, up to and including immediate termination of employment. Temporary contract workers, independent contractors, and consultants are subject to the provisions of the relevant service agreements. Any Users found to have violated this Policy may be subject to legal action by Avient, third parties, and/or governmental entities.

QUESTIONS AND ADDITIONAL INFORMATION

For additional details regarding cybersecurity and incidence response, please refer to Avient's Cyber and Data Incident Response Policy.

If you have questions about or require assistance with implementing this Policy, please contact an Avient Human Resources representative or appropriate Avient IT Representatives. By signing below, you acknowledge that you have read and intend to comply with this Policy:

Name (please print) _____

Location _____

Signature _____

Date _____

Reservation of Rights

Avient reserves the right, in its sole discretion, to amend, suspend, or terminate this Policy without prior notice to the extent permitted by law. This Policy does not create a contract of employment, and does not alter an employee's status as an at-will employee.

DOCUMENT CHANGE AND REVIEW HISTORY

Ver.	Summary of Changes	Date
	Previous version	09/30/2016
Final	Policy rewritten and simplified.	09/01/2021

APPENDIX A: DEFINITIONS

In addition to those terms defined within the body of this Policy, the following definitions are used:

"Avient Data" – includes (a) all data and information generated, stored, collected, or processed by Avient through Information Systems; (b) all information under the control of Avient and originating from, belonging to, or received from customers, suppliers, or third parties; (c) all data and information regarding intellectual property of Avient; and (d) purely intra-Avient information connected to individual employees, such as Information System usernames, passwords, and company ID.

"Personal Data" – any information relating to an identified or identifiable natural person as defined under applicable law. For example, Personal Data could be an individual's Social Security Number (SSN), name, address, date of birth, tax identification number or equivalent, credit or debit card number, or financial account number. Personal Data additionally includes any non-Avient data of a private nature, such as login information for personal email, social media, or subscription service accounts, personal documents, and notes.

"Confidential Data" – all confidential or proprietary information, including any Avient Data, Personal Data, and third party data accessible or stored on Information Systems.

"Information Systems" – any software, hardware, firmware, data networks, physical or remote storage media, or other digital services used, owned, accessed, controlled, leased, or operated by Avient. Examples of Information Systems include, but are not limited to, computer equipment (PCs, printers, copiers, monitors), storage media (USB-devices, data disks/cards, cloud storage/applications), cell and desk phones, internet access, internet servers, and operating systems.

"Users" – all Avient workers with either in-person or internet access to Information Systems, including, without limitation, employees, remote workers, temporary contract workers, independent contractors, and consultants.