

---

# EMPLOYEE HANDBOOK

---



VISCOSITY  
NORTH AMERICA

## CLIENT COMPLIANCE

Upon on-boarding, Viscosity completes a standard background check. Occasionally, a more in depth background check and/or drug screening may be required for client compliance and regulations, such as HIPPA, PCI, PHI, and SOX. Some clients may require us to perform these checks on a regular basis. Clients and Viscosity may require employees to complete compliance training as well.

### References / Employment Verification

To ensure that all reference checks are handled in a manner consistent with Viscosity's policy guidelines, all reference requests must be directed to admin@viscosityna.com as the designated authorized source for reference information. Only job title and dates of employment will be verified. Verification of salary will be provided only if the employee emails admin@viscosityna.com ahead of time with a release of information statement, or provides a signed written release letter to HR in person.

## COMMUNICATIONS POLICY

To assure that any information being shared with people outside the company is consistent, and as accurate as possible and available to all, refer any information requests to the executive management team. The executive management team will be responsible for communicating all business information about the company. Business information includes things like sales, product developments, customer contracts, hiring and firings and other major events related to the business. Viscosity employees should refrain from discussing the business of the company with anyone outside the company. Any questions about this policy should be directed to the Director of Operations or Viscosity ownership for guidance.

### Weekly Status Reports

Each consultant, developer, architect, project coordinator/manager and database administrator, is responsible for submitting weekly status reports. The weekly status report is a daily account of an employee's progress and accomplishments on current work assignments.

## INFORMATION SYSTEMS USAGE

Viscosity makes available to you some or all of the following equipment and software to help us deliver the best possible service to our customers:

- ❑ Desktop Computers
- ❑ Laptop Computers
- ❑ Electronic Mail (e-mail)
- ❑ Internet Access
- ❑ Printers
- ❑ Telephones
- ❑ Cellular Telephones
- ❑ Voice Mail
- ❑ Document Scanners
- ❑ USB Thumb Drives
- ❑ External Hard Drives
- ❑ Cloud Storage or File Hosting Services (DropBox, OneDrive, Google Drive, Box.com, pCloud, Sync.com, etc)

These “Information Systems” have been provided to assist you in carrying out Company business. All Viscosity Information Systems are the property of Viscosity and are to be used only for business purposes. Viscosity’s Information Systems are not for personal use.

Viscosity’s Information Systems are not private. Thus, any information you input or transmit on a Viscosity Information System can and may be reviewed by the Company without prior notice to you, even if that information is protected by your individual password. Viscosity explicitly reserves the right to access, monitor, review, copy or delete any information stored or transmitted on any Viscosity Information System at any time as the Company deems appropriate. This may include random, unannounced audits to ensure that the Company’s Information Systems are being used in accordance with this policy.

Misuse of the Company’s Information Systems will subject an employee to disciplinary action up to and including termination and/or legal action. Examples of misuse of the Company’s Information Systems are:

- ❑ Unauthorized dissemination of information that is confidential or proprietary to the Company;

- ❑ Dissemination of information that is confidential or proprietary to the Company without appropriate security measures;
- ❑ Unauthorized dissemination of Company information to non-employees or unauthorized employees;
- ❑ Viewing or disseminating obscene, pornographic, abusive, slanderous, defamatory, harassing, vulgar, threatening, and/or offensive material;
- ❑ Copying or distributing copyrighted materials in violation of copyright laws;
- ❑ Unauthorized posting of Company information on the World Wide Web, such as in "chat room" or public message boards;
- ❑ Unauthorized use of the Company's name or trademarks;
- ❑ Inappropriate personal use;
- ❑ Use that violates any other Company policy including Company policies regarding confidentiality, courtesy, solicitation, and harassment.

This list is not intended to be all-inclusive. Employees are representatives of the Company and must exercise due care not to use any Company Information System in a manner that would violate any law or reflect unfavorably on the Company.

Viscosity Information Systems are intended to assist you in performing your job. Viscosity "Information Systems" should never be shared with anyone who is not employed by the company. Viscosity, "Information Systems" should only be handled by those who need to perform their responsibility for Viscosity. Use them carefully, conservatively and courteously.

## CONFIDENTIALITY

Viscosity considers information acquired in the course of doing your job to be confidential in nature and for Company use only. This includes but is not limited to non-public information regarding Viscosity's customers, suppliers, products, sales, marketing, and financial data. "Non-Public" information means information, which has not been published by the Company or someone else, such as in a press release. Viscosity considers any inappropriate release of Company confidential information to be a serious breach of Company policy and a violation of the law.

As Viscosity shares internal toolsets and methods, we ask that you do not disclose this information with anyone outside of Viscosity. Viscosity shares pertinent documentation for our consultants to be successful including proposals, knowledge base articles, standard operating procedures, system configuration, database configuration, addendums, and exhibits that represent our intellectual property and niche in the technology industry. The

Employee shall not disclose, advertise, or publish any of Viscosity documentation without the prior written consent from Viscosity.

With certain customers, employees may have strict confidentiality requirements and non-disclosure documents that we have to adhere to and even sign as part of the on-boarding process.

## SECURITY

Security on Viscosity and customer premises is a key concern and focus. It is critical that every employee takes responsibility concerning safety and security. Always keep personal belongings in a secure location. When leaving the premises, ensure that all entrances are properly locked and secured. If you notice anything suspicious or out of the ordinary, be sure to report it immediately.

Due to the nature of Viscosity's business, information security, data privacy and encryption of sensitive data is a major concern as is access to databases and personal information. Our success is based on the trust of the consumer and manufacturer. This is a critical part of our business and violations of this privacy will not be tolerated. Any abuse of this policy will be treated very seriously and will be subject to disciplinary action, up to and including termination.

Employees may have access to customer's data including sensitive and private data. When dealing with the customer's database, consultants are expected to comply with the customer's SOX/PCI/SAS 70/FISMA/HIPAA security requirements. Employees are obligated to protect the customer data and adhere to compliance requirement that the customer requests.

Employees should NEVER copy sensitive data on to their desktop or laptop. Breach of data security can result in termination.