Seneca

Seneca Guidelines on Secure Handling of Confidential Information

Seneca is committed to protecting the security and privacy of confidential information entrusted to the College by its employees, students, external clients and partners, during the course of business. These guidelines serve to summarize the principles governing the secure handling of Seneca's confidential information. Employees/consultants found to be in violation of these guidelines, by deliberately using or otherwise compromising corporate or personal information (PI) may face disciplinary action.

Confidential Information

- Confidential information includes personal information (PI) as defined in the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and personal health information (PHI) as defined in the *Personal Health Information Protection Act*, *2004* (*PHIPA*). It also includes information that is vital to the strategic planning and operation of Seneca that, if disclosed, may cause significant or irreparable financial or reputational damage to Seneca. Examples include, but are not limited to, student records, personnel files, trade secrets, intellectual property, financial budgets, significant innovation ideas yet to be patented, data and results of significant research projects yet to be published, etc.

Scope of Access

- The "need to know" principle shall apply to all access requests for confidential information and or PI, meaning that only information that is absolutely required by the person requesting such access in order to carry out their duties as defined by their job functions will be released.
- Only information that is absolutely required by the external consultants in order to provide the goods and services as defined in the service agreement signed between Seneca and the vendor representing/employing the external consultants will be released.

Personal Information

- If PI (e.g. student name, employee ID, etc.) is within scope of access, such information shall be anonymized using masking techniques such as encryption, ID re-sequencing, etc. so that associated information (e.g. birthday, grade) cannot be linked to the identifiable individual. The only exception will be in situations in which it is absolutely necessary to provide such information in its original format, and without which, there is no alternative for the person requesting such access to carry out their duties as defined by their job functions (or in the case

of external consultants, to provide the goods and services as defined in the service agreement signed between Seneca and the vendor representing/employing the external consultants).

- Release of PI to external consultants must have written approval from the business owner (director/chair level or above), including a description of the information to be released. PI must be sent using a secure medium.

Data Protection

- Storage
    - Confidential information should not be stored on any personally owned devices or personal storage drives.
    - Confidential information must be encrypted when stored locally on a mobile device (e.g. USB drive, laptop, etc.).
    - In the event a Seneca device is not provisioned and that confidential and/or PI has to temporarily reside on a personal device (laptop, USB drive), reasonable steps must be taken to protect the information (e.g. encryption).
    - Where confidential information is to be stored/hosted externally, contractual protection must be in place to ensure that
        - such information is encrypted for the duration of the agreement and securely erased upon conclusion of the agreement or when it is no longer needed by Seneca (e.g. when the retention window of the information has expired as per applicable retention policy that governs it).
        - such information will not be used by storage service provider for any purposes other than what is needed to deliver the particular storage/hosting service unless explicit consent is obtained from Seneca
        - access to such information by personnel working for the storage service provider is limited to those who need such access to deliver the particular storage/hosting service and such personnel must have entered into an agreement with the storage service provider requiring them to be bound by applicable privacy and confidentiality provisions
        - Seneca is the owner of its information and that the storage service provider's role is to process/store/manage it on our behalf
        - Seneca must be notified as soon as storage service provider becomes aware of a potential or actual breach of information it is hosting/storing on behalf of Seneca
        - storage service provider shall fully co-operate with Seneca in any investigation into any breaches of information it is hosting/storing on behalf of Seneca
        - if storage service provider becomes legally compelled to disclose Seneca's confidential information, it will provide Seneca with prompt notice to that effect in order to allow Seneca to seek one or more protective orders or other appropriate remedies to prevent or limit such disclosure, and shall co-operate

with Seneca and its legal counsel to the fullest extent. If such protective orders or other remedies are not obtained, storage service provider will disclose only that portion of the confidential information which it is legally compelled to disclose, only to such person or persons to which the Party is legally compelled to disclose

- Transmission
    - Confidential information must be encrypted prior to transmission through an insecure media (e.g. Internet) or via a secure transport protocol (e.g. Seneca File Transfer).
    - Confidential information cannot be sent in an email to an external email account
- Disposal
    - External consultants who have control or custody of Seneca confidential information stored on non-Seneca owned IT equipment must ensure their secure and irreversible deletion when such information is no longer required.
    - Any Seneca IT equipment that has confidential information stored on it must be securely wiped before disposal and a certificate of disposal must be produced.
    - In accordance with Seneca's Privacy Policy, prior to disposing of any record or device containing personal information, the individual must submit an "Authorization for the Disposal of Personal Information" form to Seneca's Privacy Office for approval. In addition, personal information that has been used by Seneca must be retained for at least one year after use unless the individual to whom the information relates consents to its earlier disposal.

Data Access

- An authentication mechanism must be put into place to ensure that only authorized personnel can have access to confidential information.
- Access to confidential information shall be restricted to staff who require the information to carry out their duties as defined by their job functions or to external consultants who require the information to successfully provide goods and services as defined in the service agreement signed between Seneca and the vendor representing/employing the external consultants.
- Access to confidential information shall be restricted to times of the day/week where access is required.
- Only the minimum level of access to confidential information (e.g. read only) that is required by staff to carry out their duties as defined by their job functions or by external consultants to successfully provide goods and services as defined in the service agreement signed between Seneca and the vendor representing/employing the external consultants will be granted.
- Written approval from director/chair level or above is required for all confidential information requests.

Data Audit

- An audit trail shall exist to provide forensic evidence on when confidential information is accessed, by whom and from where.
- In the case of external consultants having access to confidential information, a written report setting out the name of each representative who has had access or may have access to PI in connection with the provision of goods and services as defined in the service agreement signed between Seneca and the vendor representing/employing the external consultants shall be provided by the vendor on a regular basis (at least once every 3 months) or at any other time upon Seneca's request for audit purposes.

Confidentiality Agreement

A confidentiality agreement shall be signed by Seneca employees before any access to confidential information can be granted during the course of business.

- A confidentiality agreement must be signed by the authorized Seneca representative before any access to confidential information can be granted to external consultants, a confidentiality agreement must be signed by a Seneca administrator (Chair or higher) and the external consultants and/or their representatives.

Dealing with Requests to Access Confidential Information

Below is a minimum set of questions that must be answered by the requestor and documented by the request reviewer/approver whenever a request is made to access confidential information:

- Business justification of the access request
- An itemized list of what needs to be accessed
- A list of individuals requiring access to requested information, their roles, reason for access, what they will do with the data, and if there is any specific timeframe that they'll need to have access to such data
- Proof of existence of signed confidentiality agreement if requestor is an external consultant (e.g. confirmation email from Seneca project sponsor (director/chair level or above))

Data Breach

Suspected breach of personal information must be reported immediately to the Privacy Office at privacyoffice@senecacollege.ca or 416-764-0400. Any suspected cyber breach must be reported immediately to the ITS Service Desk at servicedesk@senecacollege.ca or at 416-764-0411.

Questions

For further information, contact the IT Security and Compliance Office at itso@senecacollege.ca or the Privacy Office at privacyoffice@senecacollege.ca or at 416-764-0400.