Newcomp Analytics Inc.

Information Protection & Security Policy

2020

Table of Contents

Policy Statement

Newcomp Analytics will ensure the protection of all information assets within the custody of the business and our clients. This includes protecting the following information:

- Customer data in any form (electronic, or other formats including paper files or verbal information)
- Customer records (including contact and company information, sales history and passwords)
- Contact lists
- Employee Information (including email addresses and passwords)
- Company banking information
- Payment Information

High standards of confidentiality, integrity, and availability of information will be maintained at all times.

Purpose

Information is a major asset that Newcomp Analytics has a responsibility and requirement to protect.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the organization maintains. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them.

This Information Protection Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets at Newcomp Analytics. The policy specifies the means of information handling and transfers within the business.

Scope

This Information Protection Policy applies to all the systems, people and business processes that make up the Newcomp Analytics' information systems. This includes all Executives, Departments, Partners, Employees, contractual third parties and agents of the Organization who have access to Information Systems or information used for Newcomp Analytics' purposes.

Definition

This policy should be applied whenever Business Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper
- Data stored electronically
- Communications sent by mail or using electronic means

- Stored tape, video or speech

Risks

Newcomp Analytics recognizes that there are risks associated with users accessing and handling information in order to conduct official business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents
- Inadequate destruction of data
- The loss of direct control of user access to information systems and facilities
- Theft and deliberate attacks on systems and individuals who have access to sensitive data
- Inadvertent exposure due to loss of media, or information being misplaced
- Neglect to delete sensitive information when equipment is recycled, or to protect systems with a strong password or with encryption
- Insecure practices due to collecting, storing, sending, encrypting, finding, and removing data

Non-compliance with this policy could have a significant effect on the efficient operation of the organization and our clients and may result in financial loss and an inability to provide necessary services.

Applying the Policy

For information on how to apply this policy, employees are advised to refer to Appendix 1.

Policy Compliance

If any user is found to have breached this policy, they may be subject to Newcomp Analytics' disciplinary procedure. If a criminal offense is considered to have been committed further action may be taken to assist in the prosecution of the offender(s) under the Canadian Criminal Code (or applicable regional legal jurisdiction).

If you do not understand the implications of this policy or how it may apply to you, seek advice from Andrew Trotta, CFO & Legal Counsel (Newcomp Analytics).

Policy Governance

The following statement identifies who within Newcomp Analytics is Accountable, Responsible, Informed or Consulted with regards to this policy.

Andrew Trotta, CFO & Legal Counsel, Newcomp Analytics – atrotta@newcomp.com; 416-873-4639

The following definitions apply:

- **Responsible** – the person responsible for developing and implementing the policy
- **Accountable** – the person who has ultimate accountability and authority for the policy

- **Consulted** – the person to be consulted prior to final policy implementation or amendment
- **Informed** – the person to be informed after a policy implementation or amendment

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by Mike Roberts, Practice Lead & Security Officer, Newcomp Analytics (mroberts@newcomp.com ; 289-221-3876).

Key Messages

- Newcomp Analytics must draw up and maintain inventories of all important information assets
- Security awareness should be conducted as an on-going program to ensure that training and knowledge is not just delivered as an annual activity, rather it is used to maintain a high level of security awareness on a daily basis
- The following cyber security goals are critical to Newcomp Analytics' business:
    - **Confidentiality:** Any important information you have (such as employee, client or financial records) should be kept confidential. This information should only be accessed by people (or systems) that you have given permission to do so.
    - **Integrity:** Employees need to make sure to maintain the integrity of this information and other assets (such as software) in order to keep everything complete, intact and uncorrupted.
    - **Availability:** Employees should maintain the availability of systems (such as networks), services and information when required by the business or its clients.
- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the policies outlined in this document
- Users should not be allowed to access information until the Information Security Officers (Mike Roberts or Andrew Trotta) are satisfied that they understand and agree the legislated responsibilities for the information that they will be handling
- Protected information must not be disclosed to any other person or organization
- Disclosing private company information or any client's classified information to any external organization is also prohibited

Appendix 1

A1 Applying the Policy

A1.1 Information Asset Management

A1.1.1 Identifying Information Assets

The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the following:

- Filing cabinets and stores containing paper records
- Computer databases
- Data files and folders
- Software licenses
- Physical assets (computer equipment and accessories, PDAs, cell phones)
- Key services
- Key people
- Intangible assets such as reputation and brand

A1.1.2 Classifying Information

On creation, all information assets must be assessed and classified by the owner according to their content. At a minimum all information assets must be classified and labelled. The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification.

Personal Information

Personal information is any information about any living, identifiable individual. The business is legally responsible for it. Its storage, protection, and use are governed by the data protection regime in Canada.

This act is governed by the following four private sector privacy statutes: (i) the Federal Personal Information Protection and Electronic Documents Act (PIPEDA); (ii) Alberta's Personal Information Protection Act; (iii) British Columbia's Personal Information Protection Act; and (iv) Québec's An Act Respecting the Protection of Personal Information in the Private Sector (collectively, Canadian Privacy Statutes).

A1.1.3 Assigning Asset Owners

All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it should be formalized and agreed.

A1.1.4 Unclassified Information Assets

Items of information that have no security classification and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned to each department to ensure that this is complete.

A1.1.5 Information Assets with Short Term or Localized Use

For new documents that have a specific, short-term localized use, the creator of the document will be the originator. This includes letters, spreadsheets and reports created by staff. All staff must be informed of their responsibility for the documents they create.

A1.1.6 Corporate Information Assets

For information assets whose use throughout the organization is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated and the responsibility clearly documented. This should be the person who has the most control over the information.

A1.1.7 Acceptable Use of Information Assets

Newcomp Analytics must circulate the Information Protection Security Policy to all employees. This applies to all Newcomp Analytics Executives, Committees, Departments, Partners, Employees, contractual third parties and agents of the business. Use of the system is conditional on acceptance of the Information Protection Security Policy. This requirement must be formally agreed and auditable.

A1.2 Information Storage

All electronic information will be stored in centralized facilities to allow regular backups to take place. Records management and retention guidance will be followed.

Staff should not be allowed to access information until they understand and agree to the legislated responsibilities for the information that they will be handling.

Databases holding personal information will have a defined security and system management procedure for the records and documentation.

This documentation will include a clear statement as to the use, or planned use of the personal information. Files which are identified as a potential security risk should only be stored in secure network areas.

A1.3 Disclosure of Information

A1.3.1 Sharing Information with other Organizations

Protected information **must not** be disclosed to any other person or organization via any insecure method including, but not limited, to the following:

- Paper-based methods, fax or telephone

Where information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Protocol and/or Data Exchange Agreement.

If any protected information is disclosed in a way that could be harmful to Newcomp Analytics' interests or our clients, it should be reported to Mike Roberts or Andrew Trotta, and the person may be subject to disciplinary procedure.

Any sharing or transfer of information with other organizations must comply with all Newcomp Analytics requirements. In particular, this must be compliant with the data protection regime in Canada, which is governed by the following four private sector privacy statutes: (i) the Federal Personal Information Protection and Electronic Documents Act (PIPEDA); (ii) Alberta's Personal Information Protection Act; (iii) British Columbia's Personal Information Protection Act; and (iv)

Québec's An Act Respecting the Protection of Personal Information in the Private Sector (collectively, Canadian Privacy Statutes).

A1.4 Cyber Security

A1.4.1 Web Security

Below are Newcomp Analytics' Web Security considerations:

- Please seek permission when downloading new programs and ensure software is safe to install on your computer beforehand
- When someone outside of Newcomp Analytics requests any personal or business information, verify that they are a safe person to send the information to (depending on the nature of the information)
- Ensure that you are downloading from safe websites
- Ensure that any company information shared does not include any private information (this statement also applies to posting online, e.g. to social media)
- Update all of your business software when you receive notifications to do so, so that all security fixes are up to date
- Ensure that you have complex passwords that include letters, numbers and symbols
- Always be suspicious of phone calls, emails or other communications from an unknown source

A1.4.2 Email Security

It is important to follow proper email security guidelines, as email is Newcomp Analytics' primary form of communication. Below are Newcomp Analytics' Email Security considerations:

- Do not answer suspicious emails or provide any confidential information requested in emails even if they appear legitimate – if you are uncertain, please speak to a supervisor
- Do not click on any links in suspicious emails
- Do not forward the email to others – if you need to show it to a supervisor, please ask them to come and see it on your screen or print it out
- If a suspicious email appears to be from a recognized organization or client, contact the legitimate client or organization through another means of communication (e.g., by phone) and ask if they sent such an email

A1.4.3 Data Security

Below are Newcomp Analytics' Data Security considerations:

- Frequently back up your data to an external hard drive, server and/or online service – having multiple backups of your data is key in case of the failure of one of them (e.g. Google Drive)
- Download or purchase automatic backup software to ensure timed backups of your system(s)
- Store your physical backups (e.g., external hard drive) offsite in a safe place
- Newcomp Analytics' consultants are required to bring home their laptops each night to ensure that no client information is compromised
- Have emergency system boot USB sticks prepared in case of a system crash
- Properly label any sensitive information you have to ensure secure handling
- When disposing of your data, thoroughly destroy it using our paper shredding system to ensure that no information could potentially be gathered and used to harm you

A1.4.4 Remote Access Security

Below are Newcomp Analytics' Remote Access Security considerations:

- Conduct your remote computing through a Virtual Private Network (VPN)
- Limit access to your network to authorized personnel with a clear business need
- When working from home, properly secure your Wi-Fi before using your VPN
- Do not use unsecure Wi-Fi connections when travelling

A1.4.5 Mobile Device Security

Below are Newcomp Analytics' Mobile Device Security considerations:

- Ensure that all of your mobile business devices (phones, tablets) have system access passwords and are locked when not in use
- Properly safeguard data on work mobile devices
- Encrypt any sensitive data on portable storage devices

Information Protection Security Policy Agreement

EMPLOYEE NAME agrees that any intellectual property (e.g. solutions, programs, codes, drawings, methods, techniques, products) developed during the term of employment are considered the exclusive property of Newcomp Analytics Inc. or their respective client.

EMPLOYEE NAME agrees that they will not disclose any proprietary information regarding Newcomp Analytics Inc.'s client projects, business practices, financial and organizational information during or following employment with Newcomp Analytics Inc. for an unlimited time.

EMPLOYEE NAME agrees that any client mandated Non-Disclosure Agreements signed between Newcomp Analytics Inc. and the respective client must be upheld during the term of employment and for an unlimited time following termination of employment.

Any exemptions to this agreement must be made in written form and agreed to by both parties. This agreement shall be governed and construed in accordance with the laws of the Province of Ontario.

I have read and understand this agreement, and I accept and agree to all of its terms and conditions.

_____ _____

Employee's Signature Date

_____

Employee's Name (Please Print)

_____

Signature of Authorized Newcomp Signatory