Environics Analytics

Internal Privacy Policy

Jan 28, 2023

Version 3.0

Canada & US

To: Environics Analytics Staff

Policy Acknowledgement

I acknowledge that it is my responsibility to read, understand, and abide by the Environics Analytics Internal Privacy Policy.

I understand that the latest revised policy document supersedes all other data and security policies issued by the Company previously.

I am aware that I can discuss any questions I may have about the documents with my manager or any individual in the Privacy Office.

Version Control

This version was developed to satisfy the provisions of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), substantially similar provincial privacy laws (Alberta - Personal Information Protection Act, British Columbia - Personal Information Protection Act, and Quebec - Act Respecting the Protection of Personal Information in the Private Sector), Canada's Anti-Spam Legislation (CASL), Gramm-Leach-Bliley Act (GBLA), the Health Insurance Portability and Accountability Act (HIPAA), US state and federal privacy laws, and the General Data Protection Regulation (GDPR) in the European Union.

Version Number 1.0	12/12/2003
Version Number 2.0	12/2/2016*
Version Number 2.0	03/03/2017
Version Number 2.1	04/06/2018
Version Number 2.1	09/26/2019
Version Number 2.1	07/30/2020
Version Number 2.2	09/01/2020
Version Number 3.0	02/02/2021

* EA Privacy Officer initiated revision updates in 2016.

Revision History Summary

Date	Version	Section	Description of Changes	Initials

Approvals

This Policy is part of Environics Analytics overall Information Security Program. The Policy has been reviewed, approved, and endorsed by Environics Analytics Compliance Office and Senior Management Team.

Environics Analytics reserves the right to change or modify this policy at any time.

	Policy Role	Name	Title
1			
2			
3			
4			

APPROVER - COMPLIANCE OFFICE IS ACCOUNTABLE FOR ESTABLISHING, AND ADMINISTERING ENVIRONICS ANALYTICS PRIVACY POLICY AND SECURITY POLICY
REVIEWER – SENIOR MANAGEMENT IS RESPONSIBLE FOR REVIEWING ENVIRONICS ANALYTICS PRIVACY POLICY AND SECURITY POLICY

Table of Contents

1. Introduction

At Environics Analytics ("EA") respecting privacy is an important part of our commitment to our clients, staff and to the general public.

The objective of this Environics Analytics Privacy Policy is to promote responsible and transparent personal information management practices in a manner consistent with the provisions of the Personal Information Protection and Electronic Documents Act (Canada) and any other relevant legislation in Canada, as well as relevant legislation in the U.S. Such as, but not limited to, the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPPA), and in the EU, where applicable, under the General Data Protection Regulation (GDPR), and in compliance with our obligations to our clients.

This Privacy Policy governs the collection, use and disclosure of personal information in any form, whether written or electronic, by Environics Analytics including personal information held by Environics Analytics on behalf of its clients. This document explains what personal information may be collected or received and how it is used. It also explains how staff, clients or the public can ask questions, make suggestions, and express concerns about our privacy practices.

This document is aligned with the Environics Analytics Privacy Policy externally published on the EA website at http://www.environicsanalytics.ca/footer/privacy. This document is also aligned and with the Environics Analytics Master Information and Security Policy 3.0 document (known as Security Policy), which establishes EA's framework for preserving the confidentiality, integrity, and availability of information on their information systems and in those managed by service providers. References to the Security Policy can be found within this policy.

This Policy is a "living document," meaning that the document is never finished, but is continuously updated as technology, privacy and employee requirements change.

1.1 Scope

This Policy applies to all EA Staff (Environics Analytics employees, contractors, sub-contractors, consultants, temporary staff, and other workers at Environics Analytics hereafter referred to as ("EA Staff")).

This Policy applies to all information and data owned, or controlled by EA, or which EA holds on behalf of others, including but not limited to its clients, and to all assets and facilities owned, leased, licensed or managed by EA. EA "Computer Assets" being, including but not limited to, mobile phones, tablets, any other mobile computing devices, datacenters, networks, applications, web portals, databases, programs, IT infrastructure, printers, and all information content including physical copies of information.

All EA Staff must comply with this Privacy Policy. This Policy applies to all Environics Analytics businesses, functions, services, and systems.

1.2 Responsibility

The responsibility for the development and maintenance of the Privacy Policy belongs to the EA Privacy Officer or their designate. The administration and implementation of the policy are shared with the Compliance Office. Additionally, some individuals and groups have specific responsibilities under this policy as described below.

EA Staff are required to review this Policies document and sign off annually as an acknowledgement that they have read, understand, and agree to abide by the Company's Master Information Security Policy and Privacy Policy.

EA Staff are responsible for safeguarding all client & Environics Analytics information, and the physical assets that electronically or physically store that information in accordance with this Policy. Also, they are required to report any disclosure of protected information to un-authorized parties to their supervisor immediately.

Violations of Environics Analytics policies, practices, procedures, applicable laws and regulations, may result in disciplinary action, up to and including termination of employment. Local legislation, policies, and training will govern the specific disciplinary process, including criminal prosecution, where applicable.

1.3 Policy Governance

This policy is governed by the Compliance Office (CO). The CO represents a committee with strategic foresight, strategic leadership, and the responsibility to clearly define and enforce policies on behalf of the organization. The policies represent a written document outlining how to protect the organization from threats, including computer security threats, and how to handle situations when they do occur. It is also the CO's responsibility to ensure all EA Staff are kept updated on the company's security policies.

Environics Analytics reserves the right to change or modify this policy at any time to, for example, reflect any changes in policy or legislation.

1.4 Privacy and Security Awareness Training

EA shall regularly conduct awareness training regarding information privacy and security to its employees, consultants, and subcontractors. EA will conduct an annual Privacy and Security training session for EA Staff (noting, mandatory attendance is required). EA will conduct Privacy and Security training session as orientation training with new EA Staff (noting, mandatory attendance is required). The training will include code of conduct requirements, and a quiz to increase EA Staff privacy know-how. The training and testing materials will be reviewed and updated on an annual basis.

In addition, EA will conduct role specific training on Personal Information Access, Privacy Laws (CASL, Quebec, BC, Alberta, US, EU), Privacy Principles (Data Minimization), Privacy Enhancing Technologies, De-Identification, Re-Identification Risk, Data Governance, and as requested.

2. Roles

2.1 Compliance Office (Terms of Reference)

Purpose

The Compliance Office's purpose is to reduce the risk to Environics Analytics business operations by establishing policies and guidelines that detail best practices and operational prescriptions.

The Compliance Office will represent a consolidated resource for compliance information, including privacy, security, and data governance.

Mandate

The Compliance Office will develop and implement appropriate policies and procedures to help guide EA staff on executing their corporate and strategic objectives.

Through staff security and awareness training, the Compliance Office will strive towards ensuring that corporate policies are adhered to, and overall corporate risk is minimized.

The Compliance Office will facilitate communication and education programs that will train, and inform, Environics Analytics staff of pertinent laws, regulations, and corporate policies.

Using a risk-based approach, the Compliance Office will provide continuous monitoring and assistance regarding compliance assurance activities.

Membership

The Compliance Office is comprised of Subject Matter Experts representing specific departments and functions within the business. The members of the committee are selected and de-selected by the Chair. Term. Committee members have an indefinite term.

- Chief Executive Officer and Chair*
- Corporate Services Subject Matter Expert
- Business and Strategy
- Sales
- Privacy
- Risk
- Human Resources
- Product Management
- Project Management
- Information Technology
- Security
- Data Governance
- Legal, Contracts
- Data Modelling and Analytic Services
- Data Build Automation
- Compliance Officer **

Note1* The Chair of the Compliance Office is charged with providing leadership and direction of the committee.

Note2** The Compliance Officer is the Compliance Office secretary responsible for the documentation and communication of the activities of the committee.

Responsibilities

- The Compliance Office identifies risks that an organization faces and advises on how to avoid or address them.
- The Compliance Office monitors and reports on the effectiveness of controls in the management of the organizations risk exposure.
- The Compliance Office resolves compliance issues and advises the business on rules and controls.
- The Compliance Office approves the Master Information and Security Policy, and the Privacy Policy.

Meetings

Frequency: Monthly. If the Compliance Office is unable to meet, then a report will be distributed in its stead. Also, a meeting can be called by a committee member, The Chair or Secretary at any time.

Quorum: A simple majority of the Compliance Office in attendance will constitute a quorum.

Decision Making: All members can vote, and decisions will be based on Consensus (majority of the participants in agreement, with a minority of objections).

Agenda: The Secretary will distribute the agenda prior to the meeting. The topics for discussion include Compliance, Policy, Privacy, Security, Risk, Data Governance and Audit. The format can change to accommodate business objectives.

Minutes: The Secretary, or an appointed delegate, will record the minutes of each meeting. The meeting minutes will be circulated to the Compliance Office after the session has concluded.

2.2 Environics Analytics Senior Management Team (EASMT).

Consists of all Senior Executives (Titled Senior Vice Presidents and above) within EA Staff. Regarding this policy, EASMT is responsible for:

- Reviewing, and editing Policy
- Ensuring that EA Staff understand and follow this policy and referenced work instructions
- Ensuring that EA Staff appropriately protect information assets and physical property
- Ensuring that EA Staff immediately report any risk items and disclosures of protected information to unauthorized parties

2.3 Privacy Officer

The role of the Privacy Officer (or access and privacy officer/coordinator) would generally include:

- Ensuring that the organization implements and complies with relevant Privacy Laws.
- Establishing and implementing privacy management program with controls, including creating privacy policies and procedures, as well as designing and implementing employee training
- Ongoing assessment and revision of program controls
- Representing the organization in the event of an investigation
- Demonstrating leadership within the organization in creating and maintaining the desired culture of privacy
- Ensuring Privacy Officer's contact information is published on the organization's website

- Participate in the conduct of Privacy Impact Assessments ("PIAs") involving certain information systems or electronic service delivery systems and suggest measures to ensure the protection of personal information processed in connection with such systems.
- Receive and respond to access and rectification requests as well as requests related to data portability and the right to be forgotten.

The role of the Privacy Officer should be clearly communicated throughout the organization and supported by senior management.

2.4 Environics Analytics Staff (EA Staff)

Privacy is everyone's responsibility. It is incumbent for all EA Staff with access to Environics Analytics information to protect it accordingly and to abide by the Privacy Policies. EA Staff shall comply with the Security Policies, including the maintenance of data confidentiality. Failure to do so may result in disciplinary action.

3. Privacy Laws and Privacy Compliance

3.1 Compliance with Canadian Privacy Laws and US Privacy Legislation

Environics Analytics Privacy Policy is intended to promote information management practices, in a manner consistent with the provisions of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), substantially similar provincial privacy laws (Alberta - Personal Information Protection Act, British Columbia - Personal Information Protection Act, and Quebec - Act Respecting the Protection of Personal Information in the Private Sector), Canada's Anti-Spam Legislation (CASL), Gramm-Leach-Bliley Act (GBLA), the Health Insurance Portability and Accountability Act (HIPAA), US state and federal privacy laws.

3.2 Privacy Compliance & EU General Data Protection Regulation (GDPR)

Environics Analytics understands that Canada's national privacy law, PIPEDA, owes much of its origin to the 1995 EU Data Protection Directive and adopted its ten privacy principles, and the precepts of "fair information practices" as embodied in the Directive and as originally set out in the OECD's 1980 Privacy Principles.

It is also understood that that the GDPR represents an enhancement in the rigour of privacy protections that have been required in the EU under the 1995 Directive. Environics Analytics compliance programs respond to all Canadian, US and EU privacy laws as applicable to ensure that adequate privacy protections and mechanisms are in place and effective.

3.3 Privacy Principles

EA values and adheres to a comprehensive set of tools that enable EA to be an active member of the privacy community. The following are EA's privacy principles are documented on EA's external privacy policy/notice:

1. EA only uses 100% privacy compliant data as inputs for product development.
2. Personal Information provided to EA by clients is used solely for the purpose of their business and is safeguarded in client-specific firewalled locations in secured data centres.
3. Personal information that we process for any purpose or purposes is not kept longer than we determine is reasonably necessary for that purpose or those purposes.
4. EA complies with legal obligations in relation to the retention and deletion of personal data.
5. Personal Information is only to be used for the purposes to which the provider consented.
6. Personal Information held on behalf of clients is not shared with any third party under any circumstances unless there was explicit consent to the sharing.
7. No personal identifiable data is used by Environics Analytics in its data products. Data are either modeled from statistical information for other geographic aggregations using well-accepted statistical modelling techniques or are aggregations of completely anonymized data and fully conform to all privacy legislation in Canada, the United States and Europe and to all standards set by organizations such as Statistics Canada.
8. EA is SOC1, SOC2, HIPAA compliant, and TRUSTe Data Collection certified - the highest auditable standards for data processing, security and privacy.
9. EA is aligned with industry self-regulatory standards such as the DAA OBA Principles and the NAI 2018 Code of Conduct.
10. EA operates in accordance with strict privacy and security policies and procedures, consistent with Canadian, U.S. and EU privacy laws and regulations (including PIPEDA, GLBA, CCPA, GDPR).

3.4 Personal Information

The Personal Information Protection and Electronic Documents Act (PIPEDA) sets out the ground rules for how businesses subject to the law must handle personal information in the course of commercial activities. For the

purposes of this Privacy Policy, Personal Information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information, in any form, such as:

- Age, name, ID numbers, income, ethnic origin, or blood type
- Opinions, evaluations, comments, social status, or disciplinary actions
- Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs)

Reference – Office of the Privacy Commissioner of Canada website. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/#_h2

Organizations covered by PIPEDA must obtain an individual's consent when they collect, use or disclose that individual's personal information. People have the right to access their personal information held by an organization. They also have the right to challenge its accuracy. Personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, they must obtain consent again. Personal information must be protected by appropriate safeguards.

3.5 Privacy Management Program

EA will develop and maintain a Privacy Management Program (PMP). The program will be led by EA's Privacy Officer, who is appointed to oversee the development, implementation, and maintenance of the program. An accountable organization must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a Privacy Management Program.

The Privacy Officer will develop an oversight plan to review the Privacy Management Program periodically. The plan would set out a schedule of when policies and other program controls will be reviewed. This will include documented privacy assessments associated with changes to the EA operating environment, new data products, and relevant organizational changes (such as duties, statutory or policy framework, organizational or management structures). The plan includes a schedule of when all policies and other program controls will be reviewed.

The Privacy Officer will follow the duties of a Privacy Officer, and ensure Internal policies are in place such as:

- Collection, use and disclosure of personal information, which include requirements for consent and notification
- Access to and correction of personal information
- Retention and disposal of personal information
- Responsible use of information and information technology, including administrative, physical and technological security controls and role-based access
- Data Breach Reporting
- Challenging compliance

The PMP will ensure EA is able to identify: the personal information in its custody or control, its authority for the collection, use and disclosure of the personal information, and the sensitivity of the information. The personal information inventory and associated data flows will be documented by the Data Governance Office.

The program must adapt to keep current with changes in services, administrative structures, and applicable legislation. EA will review and revise their privacy management program on an ongoing basis and ensure privacy

management is part of the organization's routine operational tasks. A solid PMP ensures that privacy is built into all company initiatives, programs, or services.

An effective PMP will incorporate different types of reporting mechanisms to ensure the privacy officer and senior management are informed, on a regular basis, whether the privacy management program is functioning as expected, and if not, of the proposed fixes. EA will execute an annual review of the program, and report to the Compliance Office Chair the results of the review.

The PMP will establish processes to respond to requests from individuals for access to (and correction of) their personal information, and the need to be able to respond to complaints from individuals about how personal information is being protected.

As identified in the Quebec's Privacy Law (ACT RESPECTING THE PROTECTION OF PERSONAL INFORMATION IN THE PRIVATE SECTOR), EA will inform, on request, the individual of: (i) the personal information collected from them, (ii) the categories of employees who have access to the information within the organization, (iii) the duration of the period of time the information will be kept; and (iv) the contact information of the Privacy Officer. When collecting information from another organization, an organization must, at the request of the individual, inform them of the source of the information (unless this information is part of an investigative file established for the purpose of preventing, detecting or repressing a crime or an offence under the law).

The PMP will require all EA Staff to be aware of, and be ready to act on, privacy obligations. Up-to-date training and education requirements for all employees, tailored to specific needs, are key to the success of the PMP, and the Compliance Office.

Risk Assessments should be conducted for all new services, programs or systems involving personal information, or when significant changes are made to existing ones. Assessment tools, such as Privacy Impact Assessments (PIAs) and Vendor Risk Assessments can help identify and repair associated incidents, or prevent them from arising in the first place.

The PMP will ensure that privacy provisions will be included in contracts, setting out requirements for compliance including binding the service providers, partners, and clients to privacy legislation, the policies, and protocols of EA.

A successful PMP will require executive support. The Compliance Office, and EASMT are committed to supporting EA's PMP. Senior management endorses the program controls, the role of the Privacy Officer and provides necessary resources to effectively operate the Privacy Management Program.

The PMP will ensure the organization is transparent about the measures EA has taken to protect personal information. EA will provide enough information so that the public knows the purpose of the collection, use and disclosure of personal information as well as how it is safeguarded and how long it will be retained.

EA will implement administrative, technical, and physical safeguards to protect all personal information.

EA PMP will align with principles set out in Privacy by Design. The objectives of Privacy by Design is to ensure privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage, may be accomplished by practicing the following 7 Foundational Principles referenced here https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

1 Proactive not Reactive
2 Privacy as the Default Setting
3 Privacy Embedded into the Design
4 Full Functionality
5 End-to-End Security
6 Visibility and Transparency
7 Respect for User Privacy

An effective Privacy Management Program will be able to identify an organizations weaknesses, strengthen their good practices, demonstrate due diligence, and potentially raise the protection of personal information that they hold to a higher level than the bare minimum needed to meet legislative requirements. In general, the effectiveness of the program, and program controls must be monitored and periodically audited and revised, where necessary.

Reference for *Getting Accountability Right with your Privacy Management Program* can be found here https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/

3.6 Data Sources and Data Products

Environics Analytics obtains privacy-compliant de-identified or anonymized data from trusted data partners. Data such as the latest census data, current economic indicators, postcensal estimates from federal and provincial governments, immigration statistics, economic data such as building permits, survey data, life stage data, certain location data and business-to-business data. This data may have been originally collected either online or offline.

In general for traditional products, the data collected would be geo-demographic or survey data at the postal code or dissemination area (DA) level in Canada, or general demographic data. The data represents a number of households and/or population at a geography level. From time to time, U.S. customers may send EA ZIP+4 address information for the purpose of appending anonymous demographic cluster information to the addresses before it is returned to them.

The data product Demostats represents a proprietary database created using innovative methods that combine econometric, demographic, and geographic models. The product, with 750 variables, was developed primarily with CensusPlus as the core input, with some data variables sourced from Equifax. The data is anonymized and aggregated by Equifax Inc. at the source and no personally identifiable data is provided to the EA. DemoStats variables are available at the six-digit postal code level (FSALDUs) for current-year estimates and the dissemination area (DA) level for future-year projections.

EA's Neighbourhood View data product is a database updated quarterly. It includes 198 variables that have been grouped into four themes; the data is available at the postal code level and all higher levels of geography. Neighbourhood View is sourced as a dataset developed by Equifax to help marketers locate neighbourhoods that contain higher concentrations of consumers who have desirable credit characteristics and who would be more likely to consume a company's products. Neighbourhood View from Environics Analytics (EA) is an aggregated, privacy-compliant product.

Environics Analytics MobileScapes data product represents privacy-compliant and anonymized mobile movement data collected by our trusted suppliers from permission-based apps that are location-enabled on mobile devices.

The location-enabled mobile data is collected only if permission is provided by the individual. Consumers can easily change their level of location sharing overall or for individual mobile apps at any time via their privacy settings on their mobile devices. Depending on the individual app settings, device holders can decide if a particular app should share their location while in use or block that permission outright. For more information on how users can change their preferences, please see https://www.networkadvertising.org/mobile-choice

The data elements received by EA by our trusted suppliers are advertising identifiers along with a date, time and latitude/longitude coordinates for each observation. For any location data that could identify an individual, the data elements are adjusted or aggregated to render them non PI or de-identified. For clarity, the collection and use of data from trusted third-party data partners, their websites, and applications are subject to those data providers' privacy policies and legal terms.

To learn more about the privacy practices of our key third-party service providers please see the links below:

- Statistics Canada https://www.statcan.gc.ca/eng/reference/privacy/personal-info
- Equifax https://www.consumer.equifax.ca/privacy/
- Spectus – AI Privacy Center https://spectus.ai/privacy/
- Near https://near.org/privacy/
- VeraSet LLC https://www.veraset.com/privacy-policy

EA endeavors to work with providers, clients, and partners that provide disclosures to their own users regarding their use of data for marketing, interest-based advertising purposes and available privacy controls. EA will only be able to directly apply controls to the data that it possesses and manages. EA reserves the right to change data sources at any time.

3.7 Consumer List Products – Canada

Environics Analytics, in Canada, licenses Personal Information to clients that have been sourced from the publicly available telephone directory listings mentioned above or alternatively may use such information for clients who have provided Personal Information to EA for analytic or modeling purposes. This use of the Personal Information is strictly limited to the identified purpose and its use, disclosure, and retention are governed by contractual provisions. In addition, EA will have personal information, used in accordance with this policy and any applicable laws, of individuals who communicate directly with EA.

In the case of telephone directory listings, we may make them available to clients for marketing purposes such as telemarketing or direct mail. In addition, we may use statistical models to search the databases, which may contain information for a given geographic area such as the postal code, or zip code, possibly including, but not limited to average age, average income, median home value, modeled ethnicity, etc. Please note that in these geographically based query situations, EA does not have any personally identifiable information beyond name, address and phone numbers as all other attributes are applied at the neighborhood level.

In the U.S., Environics Analytics does not license personal information to clients and does not make U.S. telephone directory listings available to U.S. clients.

3.8 Client Data

EA may receive the personally identifiable information (PII) of clients' customers for analytic or modeling purposes on behalf of the client. The use of PII is strictly limited to the purpose identified by the client and its use, disclosure and retention are governed by contractual provisions as well as U.S. and Canadian privacy laws.

EA limits personal information collection (whether directly or through the use of third parties) to the specific data reasonably useful for the purpose for which it was collected.

3.9 Meaningful Consent

Meaningful consent is an essential element of Canadian private sector privacy legislation. Under privacy laws, organizations are generally required to obtain meaningful consent for the collection, use and disclosure of personal information.

Article 14 of the Act respecting the protection of personal information in the private sector states "Consent to the collection, communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes". Such consent is valid only for the length of time needed to achieve the purposes for which it was requested, and when a request for consent is made in writing, the organization must ensure that the request is presented separately from any other information communicated to the individual.

The Office of the Privacy Commission published seven guiding principles for meaningful consent, in which Environics Analytics will follow.

1. Emphasize key elements
2. Allow individuals to control the level of detail they get and when
3. Provide individuals with clear options to say 'yes' or 'no'
4. Be innovative and creative
5. Consider the consumer's perspective
6. Make consent a dynamic and ongoing process
7. Be accountable: Stand ready to demonstrate compliance

Environics Analytics will conduct role-based training on the subject of consent.

3.10 Privacy Enhancing Technology

Privacy Enhancing Technologies, or PETS, are technologies that have been bred out of necessity to preserve the privacy of individuals, while allowing meaningful, and sometimes life saving, insights to be drawn from data sets that have been traditionally hard to share.

They are used to protect individual rights, while still allowing business operations to continue. Where in the past, personal data would be exchanged between companies, PETs can limit this exchange to only what is absolutely necessary.

Environics Analytics uses Privacy Enhancing Technologies during our modeling processes to ensure that our data products do not contain any personal information, and the data cannot be re-identified to identify the data subjects. Techniques or mechanisms EA executes include Data smoothing, estimation of sub-DA level statistics, creation of segmentation and classification systems, LDU estimation of a behaviour or attribute, Data Governance (DG), Encryption, Data De-Identification and Anonymization, Technical Enforcement, Data Isolation, Data Classification, DGO Data Tracking, DGO Data Destruction and Data Minimization.

3.11 Data Minimization

Data minimization is a fundamental privacy design principle which requires that services and applications only process the minimum amount of information strictly necessary for the service or for a particular transaction. Our

objective is to minimize the amount of personal information collected and used by online service providers (e.g., to mitigate the risk of profiling based on user behaviour). EA applies this process at multiple levels.

- Gate keeping checks that are executed from the moment that we meet a potential supplier, until a final product is delivered to our clients
- Minimal selection of data at the time of request and with the DGO during inflow management.
- The DGO and associated business department collaborate on required data during the inflow stage.

Environics Analytics will conduct role-based training on the subject of Privacy Enhancing Technology.

3.12 Re-identification Risk

Re-Identification is any process that re-establishes the link between De-Identified information and an individual. Re-identification Risk is the risk that de-identified records can be re-identified. EA Privacy Office executes Privacy Impact Assessments (PIA) to determine the risk of holding and maintaining Personal Information. As an extension to PIA process, EA Privacy Office also assesses re-identification risk. The assessment identifies if the risk in the data set is appropriately weighted against the risk to the individual if the personal information data were to be re-identified. This threshold is based on the degree that the individual's privacy would be invaded if the data were breached. The result of the assessment represents a qualitative value in the range of "low," "medium" or "high." EA follows the Information and Privacy Commissioner of Ontario De-identification Guidelines for Structured Data. Included in the assessment process, is the evaluation of attribute disclosure risk. Attribute disclosure can occur if a individual is correctly re-identified and the dataset contains variables containing information that was previously unknown.

Environics Analytics will conduct role-based training on the subject of Re-Identification Risk.

3.13 PIPEDA and Online Consent for Publicly Available Information

Under Personal Information Protection and Electronic Documents Act (PIPEDA), knowledge and consent for certain purposes are not required when information meets the definition of "publicly available.". PIPEDA Regulations define "publicly available" information as information appearing in telephone directories, professional or business directories, government registry information, records of quasi-judicial bodies and journalistic or literary publications that are available to the public. Generally speaking, no consent is required as long as the collection, use, and disclosure of such information relates directly to the purposes for which it was made publicly available (other than for telephone directories and publications). However, "publicly available information" should not be confused with "information that is accessible to the public." In fact, the definition of "publicly available" under PIPEDA is very restrictive. These are the acceptable conditions:

- "Publicly available" information also includes information published in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public and where the individual has provided the information.
- All personal information that is not "publicly available" as defined above, or which is not covered by the other exceptions, requires consent.

For further information, please refer to the OPC's Interpretation Bulletin on publicly available personal information - https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_oc_201405_faq/

3.14 Indigenous data management

EA acknowledges the importance of Indigenous data sovereignty principles that recognize and respect self-determination for First Nations, Inuit and Métis Peoples, whose traditional and ancestral territories are in Canada. It must be understood that Indigenous data must be managed in accordance with data management principles developed and approved by these communities, and on the basis of free, prior and informed consent. This includes, but is not limited to, considerations of Indigenous data sovereignty, as well as data collection, ownership, protection, use, and sharing. The principles of Ownership, Control, Access and Possession (OCAP®) are one model EA supports for First Nations data governance, the other EA recognizes are the CARE Principles for Indigenous Data Governance (Collective benefit, Authority to control, Responsibility, and Ethics), which reflect the crucial role of data in advancing Indigenous innovation and self-determination. These principles complement the existing FAIR principles encouraging open and other data movements to consider both people and purpose in their advocacy and pursuits.

EA Privacy Office will develop and execute role based Privacy and Security Training on Indigenous data management.

3.15 Third Party Processors and Service Providers

Third party processors and service providers are required by contract to comply with this Privacy Policy and with data security, retention, and stewardship standards equivalent to or higher than those adhered to by EA. There must be contractual requirements in place with service providers to protect personal information, including but not limited to, ensuring trans-border data flows and requirements of the foreign regime are addressed in service provider arrangements, as appropriate, and the sensitivity of personal information is addressed in service provider arrangements, as appropriate.

Privacy requirements for service providers include the following:

- Compliance requirements, such as binding the service provider to the policies and protocols of the organization and requiring the organization to be notified in the event of a breach
- Compliance to applicable privacy laws, such as the requirement to obtain individuals' consent to lawfully collect, use, and disclose personal information in the course of commercial activity
- Training and education for all service provider employees with access to personal information
- Restrictions on sub-contracting
- Regularly executing Vendor Risk Assessments and Audits
- Agreements with service provider employees stating that they will comply with the organization’s privacy policies and protocols

4. EA Data Governance and Data Protection

Environics Analytics Data Governance and Data Protection Policy is documented within the EA Master Information and Security policy (document). Data Governance defines how EA and client information is and, will continue to be accurate, accessible, and protected throughout its lifecycle.

4.1 Data Governance Policy

Overview

Environics Analytics Data Governance Policy describes Environics Analytics information management systems that ensure that all enterprise and client information is and will continue to be accurate, accessible, and protected throughout its lifecycle.

The policy establishes organizational responsibility for information and data under all Environics Analytics businesses, functions, services, and systems and the procedures to be used to manage it.

Purpose

The purpose of this policy document is to set out data governance practices and procedures for all Environics Analytics enterprise and client information assets.

Scope

This policy applies to all EA Staff. This policy addresses EA's Data Governance Program, which includes (but not limited to) technology, data transfer, client data handling, retention and disclosure, documentation, data training, data quality, data stewardship and training, data security breach management, monitoring, audit and change management.

Policy

4.2 Technology and Data

Environics Analytics Information Technology (EAIT) and the EA Data Governance Office (DGO) is responsible for delivering and supporting the systems, services, and information technology infrastructure required to manage and use all data and information. EAIT performs generally accepted system administration tasks, including physical site security, monitoring equipment, administration of security and authorization systems, backup and recovery procedures, capacity planning, and system performance monitoring.

4.3 Data Stewardship and Training

The stewardship plan is to engage all stewards and subsequently, their departments with taking care of data assets. Data stewards assigned within each functional group are to provide data governance support to their co-workers and to provide subject matter expertise and feedback to the data governance office. The request if for all data-related work to be performed according to policies and practices as established through governance.

4.4 Information and Data Transfers

Environics Analytics works with clients to ensure that information and data is transmitted with the utmost security. Transmission processes can be found in the Information and Classification Policy within the Security Policies. The DGO manages the Secure File Transfer Protocol (SFTP) controls.

4.5 Data Inventory

All client data files collected (inbound) by EA will be logged by the Data Governance Office (DGO). The DGO will record where the data resides on the EA network. As well, the DGO will update associated workflow and data flow documentation.

4.6 Retention and Destruction

Retention and destruction of enterprise information are determined by enterprise use requirements and data retention policies. Retention and destruction of client information are determined by client requirements. If a client or supplier does not require their data retained, we request to be informed of these exceptions before Environics Analytics receives any data.

4.7 Data De-identification and Data Anonymization

For the purposes of this policy, we have defined De-Identification and Data Anonymization based on Quebec Privacy Law - *Act Respecting the Protection of Personal Information in the Private Sector*, and recently proposed *Canadian Federal Consumer Privacy Protection Act* (CPPA).

De-identification - Bill 64 provides that personal information is de-identified if it no longer allows the individual to be directly identified, requiring the removal of direct identifiers. "De-identification," which is any method that ensures that personal information "no longer allows the person concerned to be directly identified".

De-identified information is information for which the risk of re-identifying the individual is significantly reduced or eliminated in the context in which it is to be used.

Anonymization - Bill 64 states "Anonymization," which is any method that ensures that information about an individual "no longer allows the person to be identified directly or indirectly" in accordance with "generally accepted best practices". Anonymized data requires that the individual be irreversibly no longer identifiable, both directly and indirectly, thus requiring the removal of both direct identifiers and indirect identifiers.

Anonymized information is information which cannot be re-identified in any context.

The EA Data Governance Office (DGO) will document and guide EA Staff on the execution of processes associated with de-identification, data anonymization, and pseudonymization or any other similar mechanisms.

For a data set to be considered de-identified, any direct identifiable information must be removed. The values of a data set may be transformed in various ways to remove any information that identifies an individual or for which there is a reasonable expectation that the information could be used, either alone or with other information, to identify an individual. Depending on the type and nature of the identifiers, different techniques may be applied. The procedure to remove any identifiable information is supported by the DGO:

1. Removal of identifiers (direct or quasi-identifier)
2. Mask identifiers (direct or quasi-identifier)
3. Measure the data risk (example - calculating the probability of re-identification)
4. Ensure that the overall risk is rated lower than or equal to the re-identification risk threshold

The responsibility for releasing a de-identified data set does not end with the completion of the process for removing any identifiable information. A robust de-identification governance process may include activities such as:

- Assigning responsibility and accountability for de-identification
- Protecting against attribute disclosure
- Ongoing and regular re-identification risk assessments
- Auditing data recipients to ensure that they are complying with the conditions of the data sharing agreement

- Examining the disclosures of overlapping data sets to ensure that the re-identification risk is not increasing with new data releases, or that potential collusion among data recipients does not increase the re-identification risk
- Maintaining transparency around the de-identification practices of the institution
- Maintaining oversight of changes in relevant regulations and legislation as well as court cases
- Developing a response process in case there has been a re-identification attack
- Ensuring that individuals performing de-identification have adequate and up-to-date tools and processes

Data Governance is an important aspect of managing and releasing any de-identified data set.

4.8 Data Process Documentation

Environics Analytics strives to maintain proper documentation to ensure that a data trail exists through accessing, retrieving, reporting, managing, and storing of data. This is achieved by managing the flow of an information system's data throughout its life cycle: from creation and initial storage to the time when it becomes obsolete or deleted. This is accomplished by the following:

- Tracking all source data imported or loaded to Environics Analytics systems and databases.
- Identify, track, and document sensitive data types such as Personal Identifiable Information (PII) data.
- Identify and document inbound data by source, date, time, received, and retention period if applicable

4.9 Data Quality

Environics Analytics Data Quality requirement is to ensure that data collected by Environics Analytics is of the highest quality to support its intended uses. This is achieved through the allocation of accountability and responsibility for data quality by all EA Staff.

4.10 Data Security Breach Management

All data breaches will be addressed by the IT Security Incident Reporting & Data Security Breach policy within this document, and the Master Information and Security Policy.

4.11 Monitoring and Audit

The DGO will conduct periodic audits of EA data governance practices and procedures. Any gaps in compliance will be addressed by the DGO and may be escalated to the Compliance Office.

4.12 Working with Client Data on Client-owned Computers

Upon request of the Client, Environics Analytics EA Staff may be required to work with Client-owned computers in order to access Client data sets and/or Client-owned networks and computing environments. In these situations, Environics Analytics Staff must take the following measures to ensure that the Client's data is protected and secure:

- It is the responsibility of EA Staff to be aware of all Client policies that apply to the Client engagement or EA's general use of the Client's computer.
- EA Staff will not connect Client-owned computers to an Environics Analytics internal network.
- If the Client-owned computer must be connected to an EA network in order to connect the Client-owned computer to the Internet for any purpose, the Client-owned computer will only be connected to an EA guest network.
- EA Staff should not move any data directly from an EA environment to a Client-owned Computer.

- If a need to transfer data arises that can only be facilitated by transferring the data directly to a Client-owned Device, any such need must be presented to the EA Data Governance Office.

4.13 Information and Data Classification Policy

Overview

Sensitive information needs protection from disclosure and unauthorized access. Information may be classified based on its level of sensitivity and handled according to its classification. Highly sensitive information must be handled securely to preserve its confidentiality.

Purpose

This policy is intended to help EA Staff in determining the relative sensitivity of the information and what information may be disclosed to people outside of Environics Analytics.

This policy establishes information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Environics Analytics Confidential information (e.g., Environics Analytics Confidential information should not be left unattended in conference rooms).

Scope

This policy applies to all EA Staff members who handle and treat sensitive information and data. All EA Staff must familiarize themselves with the classification and handling guidelines in this policy.

The information covered in these guidelines includes information that is either stored or shared via any means, such as electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing). All Environics Analytics information is classified into seven main classifications:

1. Unclassified Public
2. Business Use Only
3. Environics Analytics Proprietary
4. Client Confidential Data
5. Client Confidential Work Product
6. Environics Analytics Business Confidential Administration Data
7. Environics Analytics Business Confidential Human Resources Data

Classification Scheme

The Classification scheme below provides details on the types of categories Environics Analytics information and data are classified.

Environics Analytics data and information require measures of protection depending upon the circumstances and the nature of information and data in question.

If the classification is not immediately clear, please discuss it with management or compliance. Questions about the proper classification of a specific piece of information or these guidelines should be addressed to the Compliance Office.

Category	Description	Examples
1. Unclassified Public	Information is not confidential and can be made public without any implications for EA. This includes routine business communications and documents created as part of day-to-day activities (the majority of email correspondence). Would have minimal impact on an individual and organization due to unauthorized disclosure.	• Product brochures widely distributed • Information widely available in the public domain, including publicly accessible • EA web site areas • Sample downloads of Environics Analytics products • Marketing Material, General Product Decks, Product Features lists, Website material • Newsletters for external transmission
2. Business Use Only	Information that would adversely affect Environics Analytics if the intended recipient is unable to read. Unauthorized disclosure, modification, or destruction would not be expected to seriously affect the organization, clients, employees, or business partners.	• Invoices, Quotes • Instructional literature for clients • Pre-Sale Count reports • Spotlight Reports • Proposals, Contracts, Agreements * Exceptions, as approved by the Data Governance Office or Compliance Office.

3. Proprietary	Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in client confidence. Information integrity is vital.	• Passwords and information on corporate security procedures • Know-how used to process client information • Standard Operating Procedures used in all parts of the Company's business • All Company-developed software code, whether used internally or sold to clients • EA purchased Source Data for use in data products • Data Products
4. Client Confidential Data	Data and Information received from clients in any form for processing and storing by Environics Analytics. Production information generated by Environics Analytics for the client, such as work product output, transformed data lists, reports, and analysis. Access to this information is very restricted. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client customer data files • Any Personally Identifiable Information (PII) data • Any Personal Health Information (PHI) data • Trade Secrets • Financial Information • Source code • Sensitive Administrative or technical information
5. Client Confidential Work Product	Data and Information received from clients in any form for processing and storing by Environics Analytics. Production information generated by Environics Analytics for the client, such as work product output, transformed data lists, reports, and analysis.	• PRIZM profiles based on client data • Work Product - Maps of client customer points report • Work Product Geosummaries client customer data • Work Product being store total sales, sales by product and other store attributes, etc. • Work Product being response analysis, penetration reports, market potential reports

	Access to this information is very restricted. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Work product being personification reports, trade area reports, additional reports which include client customer data and Environics Analytics data • Work Product Statistical Models, Spatial interaction models, etc.
6. EA Business Confidential Administration Data	Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Confidential client business data and confidential contracts • Proposals, Contracts • Legal Agreements • Quotes • Invoices • Non-disclosure agreements with clients\vendors • Competitor Information • Strategy documents • Company Policies • Company business plans • Company client lists • Sensitive Administrative or technical information • Partner/supplier relationship records • Billing information • Corporate records and data including incorporation records and filings, corporate proceedings, acquisitions/corporate transactions, intellectual property rights • Asset-related data including lease records and information, license documents and information • Trade Secrets • Sensitive Administrative or technical information
7. EA Business Confidential Human	Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to	• Employment History Files • Salaries

Resources Data	manage all aspects of corporate finance. Access to this information is very restricted. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Employee Performance Development and Improvement Files • Employment Termination Records • Occupational Health and safety records • Pension information • Health insurance applications and forms • Life insurance applications and forms • Designated beneficiary information • Applications for any other employee benefit that might require medical information such as vision insurance • Requests for paid or unpaid medical leaves of absence • Family Medical and Leave FMLA reports and related applications and paperwork • Physician-signed FMLA paperwork • Documentation about the illnesses of a family member or child for whom you apply for FMLA time to provide ongoing care • Medically related leave documentation for employees who are ineligible for FMLA time off work • Physician's examinations, notes, correspondence, and recommendations • Medically related excuses for absenteeism or tardiness from a physician • Medical job restrictions with documentation from the recommending physician • Accident and injury reports, including OSHA-required documents • Workers' compensation reports of injury or illness

		• Any other form or document that contains private medical information about an employee.

Access and Storage Requirements by Classification

The following table defines the required safeguards for protecting information, data, and data collections based on their classification.

In addition to the following data security standards, any data covered by Canadian provincial, federal privacy laws, or US state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

Unclassified Public

Impact	Would have minimal impact on an individual and/or organization due to unauthorized disclosure or dissemination.
Access	No restrictions. All EA Staff
Distribution within Environics Analytics	Standard interoffice mail approved electronic mail and electronic file transmission methods.
Hardcopy Distribution outside of Environics Analytics Internal Mail	Canada Post and other public or private carriers approved electronic mail and electronic file transmission methods.
Electronic Distribution	No restrictions to approved recipients within Environics Analytics (EA Secure Network).
Storage	Keep from the view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate. It is recommended that Unclassified Data and Information should be stored on the Environics Analytics secure network.

Business Use

Impact	Potential to have a serious impact on an individual and organization due to unauthorized disclosure or dissemination.
Access	EA Staff and non-employees with signed non-disclosure agreements
Distribution within Environics Analytics	Standard interoffice mail, shared network links, and approved electronic file transmission methods (email using EA secure network).
Hardcopy Distribution outside of Environics Analytics Internal Mail	Sent via Canada Post or approved private carriers.
Electronic Distribution	No restrictions to approved recipients within Environics Analytics (EA Secure Network). To approved recipients outside of Environics Analytics premises.

	Use the Secure Transfer method. Information and data should be encrypted or sent via a private link by way of end-to-end encryption using SFTP, HTTPS, or SSL, providing the highest level of security available. Information (not data) may be sent by [ordinary] email, only if a) confidential email disclaimer is used in the body of the email, and b) it is determined to be technically not practical and reasonable in the circumstances for the recipients not to use the secure transfer method. * Proposals, Contracts, Agreements (deemed a “Business Use” exception), can only be sent by email if password encrypted. *Spotlight reports (deemed a "Business Use" exception) can be sent by email only if the client has agreed during the ordering process to assume all risks and responsibilities in receiving the reports in an unsecured manner).

Proprietary

Impact	Would have an impact on an individual and/or organization due to unauthorized disclosure or dissemination.
Access	EA Staff and non-employees with signed non-disclosure agreements.
Distribution within Environics Analytics	Standard interoffice mail, shared network links, and approved electronic file transmission methods.
Hardcopy Distribution outside of Environics Analytics Internal Mail	Sent via Canada Post or approved private carriers.
Electronic Distribution	No restrictions to approved recipients within Environics Analytics (EA Secure Network). Information and data must be encrypted or sent via a private link to approved recipients outside of Environics Analytics premises by way of end-to-end encryption using SFTP, HTTPS, or SSL, providing the highest level of security available.
Storage	Keep from the view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Physical security is applicable, and all confidential data residing on Environics Analytics computing systems is to be encrypted.

Client Confidential Data

Impact	Would result in a severe impact on an individual and/or organization due to unauthorized disclosure or dissemination.
Access	EA Staff and non-employees with signed non-disclosure agreements.
Distribution within Environics Analytics	Standard interoffice mail, shared network links and approved electronic file transmission methods.

Hardcopy Distribution outside of Environics Analytics Internal Mail	Sent via Canada Post or approved private carriers.
Electronic Distribution	No restrictions to approved recipients within Environics Analytics (EA Secure Network). Information and data, must be encrypted, received and/or sent via a private link from/to approve recipients outside of Environics Analytics premises by way of end-to-end encryption using SFTP, HTTPS, or SSL providing the highest level of security available.
Storage	Keep from the view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Physical security is applicable, and all confidential data residing on Environics Analytics computing systems is to be encrypted. Confidential Data and Information must be stored on the EA Secure Network. It must not be stored on your mobile device.

Client Confidential Work Product

Impact	Would result in a severe impact on an individual and organization due to unauthorized disclosure or dissemination.
Access	EA Staff and non-employees with signed non-disclosure agreements.
Distribution within Environics Analytics	Standard interoffice mail, shared network links, and approved electronic file transmission methods.
Hardcopy Distribution outside of Environics Analytics Internal Mail	Sent via Canada Post or approved private carriers.
Electronic distribution	No restrictions to approved recipients within Environics Analytics (EA Secure Network). To approved recipients outside of Environics Analytics premises. • Use the Secure Transfer method. Information and data should be encrypted or sent via a private link by way of end-to-end encryption using SFTP, HTTPS, or SSL providing the highest level of security available. • Information (not data) may be sent by [ordinary] email, only if a) confidential email disclaimer* is used in the body of the email, and b) email is encrypted or password-protected, and c) it is determined to be technically not practical and reasonable in the circumstances for the recipients not to use the secure transfer method.
Storage	Keep from the view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Physical security is applicable, and all confidential data residing on Environics Analytics computing systems is to be encrypted.

	Confidential Data and Information must be stored on the EA Secure Network. It must not be stored on your mobile device.

Environics Analytics Business Confidential Administration Data

Impact	Would result in a severe impact on an individual and/or organization due to unauthorized disclosure or dissemination.
Access	EA Staff and non-employees with signed non-disclosure agreements.
Distribution within Environics Analytics	Standard interoffice mail, shared network links, and approved electronic file transmission methods.
Hardcopy Distribution outside of Environics Analytics Internal Mail	Sent via Canada Post or approved private carriers.
Electronic distribution	No restrictions to approved recipients within Environics Analytics (EA Secure Network). Information and data must be encrypted or sent via a private link to approved recipients outside of Environics Analytics premises by way of end-to-end encryption using SFTP, HTTPS, or SSL providing the highest level of security available.
Storage	Keep from the view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Physical security is applicable, and all confidential data residing on Environics Analytics computing systems is to be encrypted. Confidential Data and Information must be stored on the EA Secure Network. It must not be stored on your mobile device.

Environics Analytics Business Confidential Human Resources Data

Impact	Would result in a severe impact on an individual and/or organization due to unauthorized disclosure or dissemination.
Access	EA Staff and non-employees with signed non-disclosure agreements.
Distribution within Environics Analytics	Standard interoffice mail, shared network links, and approved electronic file transmission methods.
Hardcopy Distribution outside of Environics Analytics Internal Mail	Sent via Canada Post or approved private carriers.
Electronic distribution	No restrictions to approved recipients within Environics Analytics (EA Secure Network).

	Information and data must be encrypted or sent via a private link to approved recipients outside of Environics Analytics premises by way of end-to-end encryption using SFTP, HTTPS, or SSL, providing the highest level of security available.
Storage	Keep from the view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Physical security is applicable, and all confidential data residing on Environics Analytics computing systems is to be encrypted. Confidential Data and Information must be stored on the EA Secure Network. It must not be stored on your mobile device.

4.14 Data Retention and Data Destruction Policy

Overview

Data retention policies deal with the issue of maintaining information for a pre-determined length of time. Different types of data require different lengths of retention.

Electronic data needs to be retained for certain time periods based on one of the three following criteria:

1) Legal requirements
2) Business requirements
3) Personal requirements

Purpose

The purpose of the policy is to:

- Determine how various types of information must be retained in the possession of EA Staff
- Describe procedures for:
  - Securing and retaining data
  - Archiving information
  - Destroying information at the end of a retention period
  - Handling information under litigation
- Reduce corporate risk
- Manage Data growth
- Lower total cost of storage and systems
- Provide a better understanding of regulations and outcomes of court cases
- Guide EA Staff on how to handle and destruct information

Scope

This policy applies to information in the forms of:

- Client Files and Client data
- Vendor Data
- Data Products
- Legacy Programs and Code
- EA or Client Customer Database files
- Financial and accounting files
- Marketing and sales records
- Compliance files and Policy documents
- Human resource files, including personnel and payroll files
- Material contracts
- Browser cookies
- Intranet files
- Graphics files
- Desktop faxes
- Instant messages
- Voicemail
- Word-processing files
- Spreadsheet files

NOTE: THIS POLICY DOES NOT APPLY TO EMAILS AND ATTACHMENTS. PLEASE SEE THE EMAIL RETENTION POLICY FOR GUIDELINES ON HANDLING EMAILS AND ATTACHMENTS.

Policy

Principles

To decide on the retention and destruction, we must keep these principles in mind

- Fifth CSA Privacy Principle's requirement that "personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".
- The data will be retained as long as required by the client, as per contract and/or EA authorized document.
- The data must be of value. Considerations to determine value are
    - Usable- Data must have a purpose and be relevant to today's operations
    - Used- Data was used, viewed, or accessed in the last year?
    - Used often- How often did was the data accessed?
    - Still accurate- Is the data still accurate enough for its intended purpose?
    - Impactful- Without this data, what is the impact on the client? project? business?
- The retention period is measured by the last use date of the data (e.g. record use date, payment of the invoice, date of the termination agreement, and as deemed by owner).
- The data may reside online (server, desktop, PC), or offline (tapes, offline servers)
-

Retention Periods Chart

Based on the classification of data (from the classification scheme in the Information and Data Classification Policy), data will be retained as indicated in this chart:

Category	**Retention Period**
1.Unclassified Public	Personnel Discretion. Shall not be kept for longer than is necessary. No Minimum Maximum 7 years
2. Business Use Only	Minimum of 3 years* No Maximum - Permanent
3. Proprietary	Minimum of 3 years No Maximum - Permanent
4. Client Confidential Data	Retain or destruct as per contract, Statement of Work or client communication Otherwise, Client data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. Minimum of 3 year Maximum 7 years
5. Client Confidential Work Product	Retain or Destruct as per contract Minimum of 3 years Maximum 7 years

6.Environics Analytics Business Confidential Administration Records**	Minimum of 7 years No Maximum - Permanent Note1: Census Data will be retained for a minimum of 15 years (3 iterations) Note2: A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments.
7.Environics Analytics Business Confidential Human Resources Data	Minimum of 3 years Maximum 7 years

* Data will be retained for a minimum of 3 years. One year greater than The Provincial Limitations Act Rule of (2) years for a client to file a dispute claim after the termination of an agreement or delivery of any product under an agreement.

** Exception. The Data Governance Office, or CTO may issue an exception to retention period if authorized by the Compliance Office.

Note. All information pertinent to a lawsuit must be identified and placed on "litigation hold" during litigation cases (regardless of its form: Digital, Paper, Hard Disk, or tape). All information shall be retained during such litigation hold.

.

4.15 Removable Media Policy

Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by Environics Analytics and to reduce the risk of acquiring malware infections on computers operated by Environics Analytics.

Scope

This policy covers all portable media devices capable of retaining confidential information.

Policy

All portable media must be scanned for malware before use. EAIT will assist with this process. Portable media, cell phones, tablets, any device that can copy, photograph, or electronically capture images are prohibited from capturing images of all Confidential and Restricted information without the approval of the Compliance Office.

Portable Media will not be used for computer backups and storage of confidential, proprietary, or restricted information unless a manager approves of it, in which case encryption is required.

Backup copies of data will only be created on storage devices/systems provided by EA.

EA Staff may only use Environics Analytics removable media on their work computers. Environics Analytics removable media may not be connected to, or used in, computers that are not owned or leased by Environics Analytics without the explicit permission of the CTO and/or Compliance Office. PII or Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other government agencies.

When sensitive information is stored on removable media, it must be encrypted in accordance with Environics Analytics Encryption Policy. Exceptions to this policy may be requested in writing, on a case-by-case basis to the CTO and/or Compliance Office.

4.16 Automatically Forwarded Email Policy

Overview

Environics Analytics emails contain a lot of sensitive information. An EA Staff member forwarding an email from their EA email address may disclose confidential information to an unauthorized recipient.

Purpose

This policy intends to prevent the unauthorized or inadvertent disclosure of sensitive company and client information.

Scope

This policy applies to all EA Staff regarding automatic email forwarding.

Policy

Environics Analytics must exercise utmost caution when forwarding any email from inside Environics Analytics to an outside network. Sensitive information, as defined in the Environics Analytics Privacy Policy and Information Sensitivity Policy, should not be forwarded via any means, unless that email is critical to business and is encrypted in accordance with the Encryption Policy.

4.17 Environics Analytics Email Use Policy

Overview

Emails originating from Environics Analytics email addresses form EA's corporate culture. It is essential that email communications accurately reflect both EA's culture and official policy.

Purpose

This policy defines the appropriate use of Environics Analytics email accounts.

Scope

This policy applies to all EA Staff regarding the use of any email sent from an Environics Analytics email address.

Policy

Prohibited Use

Environics Analytics email system must not be used for the creation or distribution of any disruptive or offensive messages (including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin). An EA Staff member who receives an email with this content from another EA Staff member is required to report the matter to their supervisor immediately.

Data Exchange

Data that are exchanged using Environics Analytics email system must be encrypted in accordance with the Information and Data Classification Policy.

Personal Use

- Using an Environics Analytics email address for a reasonable amount of personal emails is acceptable. The following constraints apply when using an EA email address for personal use:
- Non-work-related email must be saved in a separate folder from work-related email.
- Sending chain letters or joke emails from an Environics Analytics email account is prohibited.
- Warnings about a virus, Trojan, or other malware infestation must be approved by the Compliance Office.

*THESE RESTRICTIONS ALSO APPLY TO THE FORWARDING OF MAIL RECEIVED BY EA STAFF.

Monitoring

EA Staff must have no expectation of privacy in anything they store, send, or receive on the company's email system. Environics Analytics may monitor messages without prior notice, although Environics Analytics is not obliged to monitor email messages.

4.18 Email Retention Policy

Overview

Email is a significant source of sensitive information held by Environics Analytics. Emails often lose relevance over time, but old emails may still clutter technology and be at risk of unauthorized access.

Purpose

The Email Retention Policy is intended to help EA Staff determine what emails (sent or received) should be retained and for how long.

Scope

This policy covers information stored or shared through email or instant messaging which may be categorized into these three classifications:

Administrative Correspondence

Environics Analytics Administrative Correspondence includes clarification of established company policy. This includes Human Resources information, performance appraisal, expenses, payroll related, holidays, policies, and workplace behavior. Administrative Correspondence also refers to legal-related material such as intellectual property, business proposals, quotes, invoices, and partner agreements.

General Correspondence

Environics Analytics General Correspondence covers information related to client interaction, operational decisions of the business, requests for recommendations or review, product development, updates, and status reports. EA Staff is responsible for email retention of General Correspondence.

Ephemeral Correspondence

Environics Analytics Ephemeral Correspondence includes personal email and non-company related communications.

Policy

The duration in which the email is retained varies from a min of immediate (destroy) to a max of 7 years. Classifications and retention periods are as follows**:**

- Administrative Correspondence (7 years)
- General Correspondence (7 years)
- Ephemeral Correspondence (Retain until reviewed, then destroy)

Encrypted Communications

Environics Analytics encrypted communications should be stored in a manner consistent with Environics Analytics Information Sensitivity Policy, but in general, the information will be stored in a decrypted format.

Recovering Deleted Email via Backup Media

Environics Analytics maintains archived backup tapes. EA Staff can submit an IT ticket to retrieve an archived email.

Exceptions

Administrative, Fiscal, and General emails will be retained for a maximum of 7 years unless EA Staff has been granted an exception by the Compliance Office.

4.19 Electronic Signature Policy

Overview

Since documentation and communication have become predominantly electronic, Environics Analytics ("EA") goal is to streamline its internal and external business efforts to eliminate manually routing paper agreements. In doing so, EA has implemented an electronic signature policy in the interest of maintaining these efforts and adhering to legal requirements.

Purpose

This policy provides guidelines for the use of electronics signatures, including defining circumstances under which electronic signatures and records will be used and accepted for validating the identity of a signer in Environics Analytics ("EA") electronic documents and correspondence, and thus a substitute for traditional "wet" signatures, within the organization. This policy is developed following applicable privacy legislation and EA's internal privacy policy.

EA's electronic signature processes are managed by the legal department. In some cases, there may be a requirement to use wet signatures, the contract administrator will procure the wet-signature upon client request

Scope

This policy applies to all Environics Analytics Group/Inc employees, sub-contractors, interns, and any other person engaged in business with EA.

Policy

The electronic signing process authenticates signer identity, demonstrated intent to sign, clear action to sign during the process to establish intent to be bound, establishes proof of signing, and the documents are protected by the technology that can detect any subsequent changes in the document.

EA accepts digital signatures on all Software and Data Agreements, Vendor and Supplier contracts (e.g. Service Agreements, NDA's, invoices and other procurement contracts or payment documentation under this policy).

EA's Electronic Records are retained solely as necessary, to meet statutory, fiscal, contractual, administrative, and operational requirements. The legal department together with other internal departments ensure that Records for which they are responsible are accurate, complete, and are retained for the periods indicated in the Regulations, and thereafter disposed of following the Regulations.

5 Security

5.1 Security Incident and Data Breach Process

Overview

Compromises in security can potentially occur at every level of computing, from an individual's desktop computer to the largest and best-protected systems. Incidents can be accidental incursions or deliberate attempts (cyber-attacks) to break into networks. They can vary from benign to malicious in purpose or consequence. Regardless, each incident requires a thoughtful response at a level commensurate with its potential impact on the security of individuals and Environics Analytics as a whole.

Purpose

This policy guides EA staff on how to respond to IT Security Incidents that threaten the company's technology systems.

Scope

This policy applies in the event of an "IT Security Incident." An IT Security Incident is any accidental or intentional act that threatens the security of EA's technology. For example:

- Misappropriation or misuse of any sensitive and confidential information (personal information, client data, financial transactions, etc.) of individuals or clients
- Spyware, Malware, Viruses, Worms, Bots, etc., that impair the functionality of the information technology infrastructure of Environics Analytics
- Unauthorized access to computing resources, networks, or information
- Allowing information technology resources to be used to launch attacks against the resources or information of other individuals or organizations.
- Cyber-attacks targeting computer information systems, infrastructures, computer networks, or personal computer devices

For the purposes of this policy a "Data Security Breach" means: (A) the loss or misuse (by any means) of Personal Data, including, without limitation any unauthorized access or disclosure to unauthorized individuals; (B) the inadvertent, unauthorized and/or unlawful Processing, corruption, modification, transfer, sale or rental of Personal Data; or (C) any other act or omission that compromises the security, confidentiality, or integrity of Personal Data. Data Security Breach includes, without limitation, a breach resulting from or arising out of Environics Analytics internal use, processing other transmissions of Personal Data, whether between or among Environics Analytics subsidiaries and affiliates or any other person or entity acting on behalf of Company.

5.2 IT Security Incidents and Data Breach Policy

The Compliance Office, in conjunction with EAIT and the affected business area, is responsible for developing response plans for IT Security Incidents and Data Breaches. As described below, a report of any IT Security Incident or Data Breach must be forwarded to EAIT and a member of the CO. The CO will determine what actions should be taken and will decide whether an incident should be handled within the company or by external security specialists. In some cases, the Compliance Office may escalate the incident to law enforcement, Environics Analytics counsel, or other Environics Analytics officers.

5.3 Reporting and Responding to IT Security Incidents & Data Breaches

EA Staff should take all practicable immediate measures to stop any IT Security Incident or Data Breach as soon as they become aware of it.

EA Staff must report all IT Security Incidents and Data Breaches to EAIT and the Compliance Office.

- By Phone: (647) 800-1417
- By Email: compliance@environicsanalytics.com
- Through the IT Ticket System
- https://environicsanalytics.atlassian.net/servicedesk/customer/portal/1/user/login?destination=portal%2F1%2FIT-52841

Data Security Incident

Report a data Breach, phishing, viruses, malware, compromised credentials, fraud or dishonest conduct, lost or stolen computing devices, miscellaneous errors (file sent to non intended recipient), etc.

5.4 Phishing emails

Phishing emails are fraudulent emails that try to obtain sensitive information by deceiving the recipient. Senders of phishing emails are disguised as trustworthy individuals by using fraudulent accounts or email addresses.

If EA Staff is aware of a phishing attempt or finds an email to be suspicious, they must:

- Take immediate action and create an IT Ticket so the experts can start an investigation.
- NOT forward the email to anyone
- NOT click any of the links or open any attachments from the email

Forwarding the email may cause you to lose meta-data contained in the email, which can help diagnose the issue. Forwarding may also lead to someone else opening the link and exposing the company to a security risk.

5.5 Spyware, Malware, Viruses, Worms, Etc.

EA Staff is required to report incidents involving viruses, worms, etc. that constitute an "IT Security Incident" by taking immediate action and creating an IT Ticket.

The user may NOT:

- Connect to the network (disconnect immediately)
- Click on any of the links
- Forward the email to anyone

EA Staff is not required to report incidents involving viruses, worms, etc. that do not constitute IT Security Incidents. Because viruses and worms can reduce the functionality or otherwise affect the corporate computing and communication environment, individuals and information technology support professionals are expected to:

- Prevent computer equipment under their control from being infected with malicious software by the use of preventive software and monitoring, and
- Take immediate action to prevent the spread of any acquired infections from any computers under their control.

5.6 Lost and Stolen Computing Devices

EA Staff is required to report incidents involving lost and stolen computing devices such as laptops, mobile phones, tablets, and USB drives. Hackers or attackers are highly capable of using their skilled computer expertise to overcome security measures and break into EA computer systems.

EA Staff is not required to report incidents involving viruses, worms, etc. that do not constitute IT Security Incidents. Because viruses and worms can reduce the functionality or otherwise affect the corporate computing and communication environment, individuals and information technology support professionals are expected to:

- Prevent computer equipment under their control from being infected with malicious software by the use of preventive software and monitoring, and
- Take immediate action to prevent the spread of any acquired infections from any computers under their control.

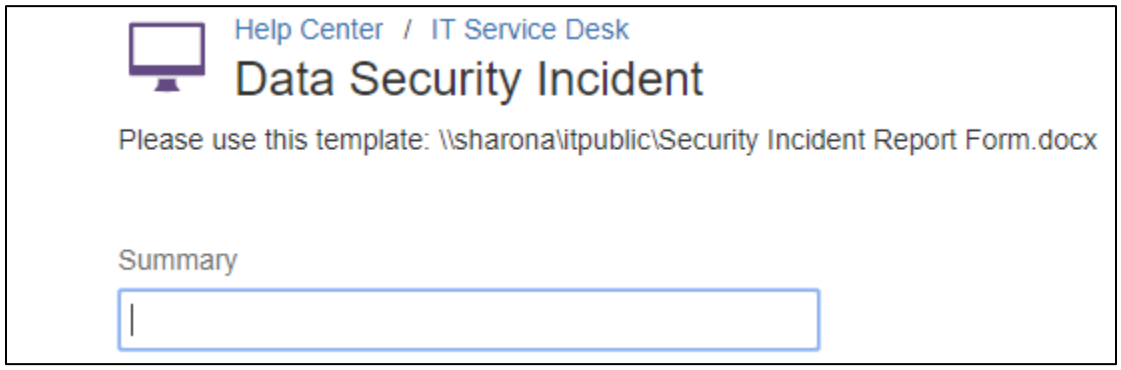
5.7 Confidential Information or data sent to the wrong recipient.

EA Staff is required to report incidents involving transmissions (electronic messages, email, fax, SFTP, hand-offs, etc.) which contain confidential or privileged information sent to persons to whom it is not addressed. Guidance to EA Staff is:

- take the time to check the TO, CC and BCC fields before initiating the transmission (i.e., pressing send)
- ensure you didn't mistakenly press 'Reply to All.'
- ensure no name substitutions have happened - you know, when you type in 'Jam' and Outlook auto-fills the name for you, so it turns out you're sending to James Smith instead of Jamie Smith.
- Be careful when attaching files. Take the extra few seconds to open the file you've attached to ensure it's the correct one and the correct version.

5.8 Security Incident Process and Data Breach Management Process

Upon identifying an IT Security Incident or Data Breach an individual must contact EAIT and the Compliance Office immediately. EAIT will require specific information to triage the incident. The information they require is an "Environics Analytics -Security Incident and Data Breach Report Form" found on the Help Desk ticket system.



A backup Security Incident form can be found on the network here \\sharona\itpublic\Security Incident Report Form.docx or here https://www.priv.gc.ca/media/4844/pipeda_pb_form_e.pdf

The form requires following items:

- the nature of the breach
- the information that was exposed
- the individuals whose information was exposed
- to whom it was exposed and how long it was created
- to whom it was exposed and how long it was exposed.

Of Note

1. If EAIT staff is unavailable and does not respond in 30 minutes, individuals may contact the CTO/VP Technology and/or email the Compliance Office Compliance@environicsanalytics.com.
2. If the incident is identified as High Risk (potentially serious consequences, or Data Breach) and requires immediate escalation, individuals should report the incident also to the CEO or CTO and/or Compliance Office (CO).
3. For Breach Containment and Preliminary Assessment. EAIT staff will assess the problem and, in conjunction with the Compliance Office determine how to proceed. Executing of techniques such as Forensics, Lineage analysis, determination of who has access, encryption Y/N, Analysis of content.
4. Following the report, individuals should comply with directions provided by EAIT support to respond to the incident, repair the system, restore service, and preserve evidence of the incident.
5. Evaluate the Risk and the Data Breach. The Compliance Office (including the CEO and Privacy Officer) will determine if the incident should be reported by executing a Data Breach Assessment (included within this policy).

The Compliance Office will document and track Environics Analytics Security Incidents and Data Security Breaches.

EAIT Support Professionals

EAIT has additional responsibilities for IT Security Incident handling and reporting. In the case of an EAIT Security Incident, EAIT support staff shall:

1. Respond quickly to the Help desk ticket from the reporting individual.
2. Take immediate action to stop the incident from continuing or recurring.
3. Repair the system, restore service, and preserve evidence of the incident.
    a. In conjunction with the CO investigate the incident to develop a response plan.
    b. Refrain from discussing the incident with others until a response plan has been formulated.
    c. follow the Compliance Office response plan to:
    d. Repair the system and restore service
    e. Preserve evidence of the incident.
4. Prevention of Future Breaches. EAIT will work to determine if the incident was benign or malicious, was data accessed or infiltrated, who was affected, the source of the breach, data types, sensitivity of the data, level of exposure.
5. Evaluate the Risk and the Data Breach. The Compliance Office (including the CEO and Privacy Officer) will determine if the incident should be reported by executing a Data Breach Assessment (included within this policy).
6. If deemed necessary by the Privacy Officer, a Post Incident Review may be conducted.

Adopted encryption technologies

- Changed password/strengthened password requirements
- Created a new/updated Security Policy
- Implemented new technical safeguards
- Implemented periodic technical and nontechnical evaluations
- Improved physical security
- Performed a new/updated Security Risk Management Policy
- Provided business associate with additional training on HIPAA requirements
- Provided individuals with free credit monitoring
- Revised business associate contracts
- Revised policies and procedures

- Sanctioned workforce members involved (including termination)
- Took (other) steps to mitigate harm.

5.9 PIPEDA Data Breach Assessment Process

1. Privacy Officer. Review the chart below to determine if the incident is a Real Risk of Significant Harm (RROSH) Risk Factor. Of note, a RROSH Risk factor of high represents foreseeable harm to affected individuals from the breach.

2. Privacy Officer. If deemed a RROSH, an Incident Report Form must be completed. The form can be found on the network. \\sharona\itpublic\Security Incident Report Form.docx or here https://www.priv.gc.ca/media/4844/pipeda_pb_form_e.pdf

3. Privacy Officer. The RROSH must logged here in the Real Risk of Significant Harm Assessment Registry .

Data Breach Assessment by Risk Factor			
Risk Factor	**Risk Level**		
	Low Risk	**Medium Risk**	**High Risk**
Nature of personal information disclosed (Assess the risk using the factors in each risk level and list information disclosed.)	Publicly available personal information not associated with any other information.	Personal information that is not: • Personal health information (as defined by PIPEDA) • Financial information • A unique government identification number	• Personal health information • Financial information • A unique government identification number
Relationships (Assess the risk using the factors in each risk level and describe the recipients and their relationship to EA.)	Inadvertent disclosure to a professional or an incorrect facility who reported the breach, confirmed no copies were made, and either: • confirmed they had deleted or destroyed the information, or • returned the documents to EA. Note: Where feasible, confirmation should be obtained by email or in writing.	Inadvertent disclosure to a stranger who reported the breach, confirmed that no copies were made, and either: • confirmed they had deleted or destroyed the information, or • returned the documents to EA Note: Where feasible, confirmation should be obtained by email or in writing.	Inadvertent disclosure to a stranger who has not provided the confirmation described in Medium Risk. Disclosure to an individual with some relationship to or knowledge of the affected individuals(s), particularly disclosures to motivated ex-partners, family members, neighbors or co-workers. Theft by a stranger.
Cause of breach (Assess the risk using the factors in each risk level and describe the cause of the breach.)	Technical or human error that was resolved or rectified.	Not applicable	Intentional breach. Cause unknown. Technical or human error that is not resolved or rectified.

Data Breach Assessment by Risk Factor			
Risk Factor	**Risk Level**		
	Low Risk	**Medium Risk**	**High Risk**
Scope (Assess the risk using the factors in each risk level and describe the individuals who are affected and how many.)	Identified and limited number of individuals (10 or less).	Not applicable	Large group or entire scope of group not identified.

Data Breach Assessment by Risk Factor			
Risk Factor	**Risk Level**		
	Low Risk	**Medium Risk**	**High Risk**
Containment efforts and follow-up actions (Assess the risk using the factors in each risk level and describe the containment efforts and follow-up actions. In all scenarios, also consider if the recipient has acknowledged the importance of keeping the disclosed information confidential.)	Privacy Office satisfied there is no risk of further disclosure as one or more of the following apply: • Data was adequately encrypted. • Portable storage device was remotely wiped and it has been confirmed that the device was not accessed prior to wiping. • Hard copy files or device were recovered and it has been confirmed that all files are intact and unread. • Information sent by secure mail and attachments opened by recipient but not saved by recipient, and item deleted from Securemail. • The recipient expressed concern for the other individual's privacy.	Information sent by email was accessed by recipient and recipient confirmed all copies of the email and all copies of attachments that were saved by the recipient were deleted from their system. Information sent by fax was accessed by recipient and recipient confirmed all copies of the fax were destroyed. Note: It is not necessary to ask an organization to delete copies of personal information that may be saved on backup systems unless there is a real risk the backup copies may be misused.	Portable storage device was remotely wiped but EA cannot confirm the device was not accessed prior to wiping. Hard copy files or device were recovered but sufficient time passed between the loss and recovery that the data could have been accessed. Information sent by email was accessed by recipient. Recipient has not confirmed deletion of all copies of the email and all copies of attachments that were saved by the recipient on their system. Data was not encrypted. Data, files or device have not been recovered. Data at risk of further disclosure, particularly through mass media or online.

Data Breach Assessment by Risk Factor			
Risk Factor	**Risk Level**		
	Low Risk	**Medium Risk**	**High Risk**
	Low Risk	**Medium Risk**	**High Risk**
Foreseeable harm to EA from the breach (Assess the overall risk using the assessment in each risk factor above and describe the foreseeable harm from the breach, including possible uses for the information.)	No foreseeable harm from breach.	Minor impacts.	Major impacts, such as: • Security risk (e.g. physical safety). • Loss of contracts or business. • Damage to reputation. • Loss of assets. • Financial exposure. • Legal action. • Major operational impacts.
Foreseeable harm to affected individuals from the breach (Assess the overall risk using the assessment in each risk factor above and describe the foreseeable harm from the breach, including possible uses for the information.)	No real risk of significant harm to an individual.	Not applicable	Real risk of significant harm to an individual, including: • Security risk (e.g. physical safety). • Identify theft or fraud risk. • Negative credit record effect. • Hurt, humiliation, damage to reputation or relationships. • Loss of business, employment, or professional opportunities. • Financial loss. • Damage to or loss of property.

Data Breach Assessment by Risk Factor			
Risk Factor	**Risk Level**		
	Low Risk	**Medium Risk**	**High Risk**
Post Incident Review (Post Mortem) (bring incident stakeholders together to discuss the details of an incident: why it happened, what impact it had, what actions were taken to resolve it, and how the team can prevent it from happening again). The results of the meeting will be documented here Real Risk of Significant Harm Assessment Registry .	If deemed necessary by the Privacy Officer, a Post Incident Review may be conducted.	Mandatory Requirement. Document lessons learned. Goal of completing a post-incident review is to learn from those incidents	Mandatory Requirement. Document lessons learned. Goal of completing a post-incident review is to learn from those incidents. Partners, clients, and other users may also want to know what happened during an outage and what steps you've taken to improve. This is be required guidance by the Office of the Privacy Commission (OPC).

5.10 Security Incident Report Form - Sample

Incident Report Forms are kept on the network \\sharona\itpublic\Security Incident Report Form.docx (on the network) and https://www.priv.gc.ca/media/4844/pipeda_pb_form_e.pdf. When reporting an incident, the individual must fill out as much information about the nature of the incident as possible.

An example of information that must be logged is as follows.

Your Information:
Your Name:
Phone (primary):
Phone (secondary):
Email Address:

Incident Information:
Discovery Date/Time:
Incident Date/Time:
The priority of Incident:
Type of Incident:
Device(s) Affected:
Operating System:

Incident Description:

Action Taken:
The nature of the breach:
The information that was exposed:
Individuals whose information was exposed (if applicable):
To whom it was exposed; and how long it was created

5.11 Quebec Data Breach Reporting Requirements

Mandatory breach reporting

If a confidentiality incident presents a "risk of serious injury," an organization will be required to take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature, which includes promptly notifying the Commission d'accès à l'information du Québec (the "CAI") and all affected individuals.

Whether a particular incident presents a "risk of serious injury" depends on the sensitivity of the information, the anticipated consequences of its use, and the likelihood that the information will be used for injurious purposes. This concept bears resemblance to the notion of breach of "security safeguards" referenced in the Personal Information Protection and Electronic Documents Act ("PIPEDA"); however, PIPEDA places greater emphasis on the likelihood of harm rather than injury.

Disclosure and record-keeping requirements under the regulation

The Regulation sets out the requirements for individual notices and reports to the CAI and details what information organizations must keep track of in their incident register.

Notice to the CAI
When: According to the Regulation, if an entity holding personal information has grounds to believe that a confidentiality incident has occurred, it must "promptly" send a written notice to the CAI.

Content: The written notice must contain the following:

1. Name of the organization affected by the confidentiality incident, along with its Québec Company Registry number;
2. Contact information of a person within the organization who can answer questions regarding the incident;
3. Description of the personal information covered by the incident or, if that information is not known, the reasons why it is impossible to provide such a description;
4. Brief description of the circumstances of the incident and what caused it, if known;
5. Date or time period when the incident occurred (or an approximation, if unknown);
6. Date or time period during which the organization became aware of the incident;
7. Number of individuals affected by the incident and the number of individuals residing in Québec (or an approximation, if unknown);
8. Description of the elements that led to the conclusion that the individuals concerned suffer from a risk of serious injury;
9. Steps the organization has taken or intends to take to notify affected individuals of the breach;
10. Steps the organization has taken or intends to take after the incident occurred, including those aimed at reducing/mitigating the risk of injury and preventing the reoccurrence of similar incidents in the future; and
11. Indication that other privacy regulators have been informed of the incident, if applicable.

Notice to the individuals concerned

When: The Regulation also provides that an organization must "promptly" send a notice to all individuals whose personal information was the subject of a confidentiality incident. This notice is sent directly to the individual concerned, unless sending such a notice is likely to cause increased injury to the individual/undue hardship for the organization and/or if the organization does not have the individual's contact information. In such cases, the organization may notify affected individuals via public notice.

Content: Similar to the written notice to the CAI, the written notice to the individuals concerned must contain the following:

1. Description of the personal information covered by the incident or, if that information is not known, the reasons why it is impossible to provide such a description;
2. Brief description of the circumstances of the incident;
3. Date or time period when the incident occurred (or an approximation, if unknown);
4. Brief description of the steps the organization has taken or intends to take after the incident occurred in order to reduce the risks of injury;
5. Measures that the organization suggests the individual concerned take in order to reduce/mitigate the risk of injury; and
6. Contact information where the individual concerned may obtain more information about the incident.

Contents of the confidentiality incidents register

What: The law mandates that organizations keep a register of confidentiality incidents, regardless of whether such incident requires notice to the CAI and/or to any individuals whose personal information was compromised. While the Regulation does not specify a format for the register, it must nonetheless be comprehensive, as organizations are required to send a copy of the register to the CAI upon request.

How long: Organizations are required to maintain records of confidentiality incidents for five years after the date or time period when the company first became aware of the incident.

Content: Much like the content of the notices described above, the register must have:

1. Description of the personal information covered by the incident or, if that information is not known, the reasons why it is impossible to provide such a description;
2. Brief description of the circumstances of the incident;
3. Date or time period when the incident occurred (or an approximation, if unknown);
4. Date or time period during which the organization became aware of the incident;
5. Number of individuals affected by the incident (or an approximation, if unknown);
6. Description of the elements that led to the conclusion that the individuals concerned suffer from a risk of serious injury;
7. If the incident presents a risk of serious injury, the transmission dates of the notices to the CAI and the individuals concerned as well as an indication of whether a public notice was required; and
8. Brief description of the steps the organization has taken or intends to take after the incident occurred in order to reduce the risks of injury.

The Confidentiality Registry can be found here on the network. For more information please see 1.1.1. Act respecting the protection of personal information in the private sector here https://www.legisquebec.gouv.qc.ca/en/document/cs/p-39.1

5.12 Security Incident and Data Breach Post-Mortem

In the event of a High Risk Security Incident or a Data Breach, the Privacy Officer will conduct a Post Mortem, review of the incident. The Privacy Officer will bring incident stakeholders together to discuss the details of an incident: why it happened, what impact it had, what actions were taken to resolve it, and how the team can prevent it from happening again. The results of the meeting will be documented here Real Risk of Significant Harm Assessment Registry .

5.13 Cyber-Security

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks.

The purpose of a Cyber Security policy is to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks, and technologies. Environics Analytics has developed, and maintains, a comprehensive Cyber Security Policy and Incident Response Plan. The policy is detailed in the EA Master Information and Security Policy, and is aligned with the National Institute of Standards and Technology (NIST) Cyber Security Framework and standards set out by the Canadian Centre for Cyber Security in their ransomware playbook ITSM.00.099. The Policy Framework is organized into five essential functions:

- Identify
- Protect
- Detect
- Respond
- Recover

In the event of a ransomware attack, the Compliance Officer, Privacy Officer and the EASMT will be responsible for engaging law enforcement, legal aid, and the Cyber Security insurance provider to coordinate the response. The EA Cyber Security Playbook can be found in the EA Business Continuity and Disaster Recovery plan.

5.14 Application development security

EA has defined, and implemented, security controls to help ensure security for application development in compliance with recognized application development standards, such as ISO 27034 Information technology, Microsoft Security Development Lifecycle, OWASP, Application Security Verification Standard (ASVS), etc. The controls include, but not be limited to, monitoring security vulnerabilities, code security reviews, approval of pre-rollout changes, developer training on secure development practices, etc.

Security test on applications and operations infrastructures

EA tests the security of deliverables and/or infrastructures and/or applications it uses to operate its technological solutions and corrects detected vulnerabilities. The tests must include vulnerability scanning and intrusion tests executed on an annual basis, or during major changes to infrastructures or applications. The tests must be carried out by qualified staff and must meet industry recognized standards (such as NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, or the Open Source Security Testing Methodology Manual)

Audit and Reports

Environics Analytics uses independent external auditors to verify its security measures for applicable privacy, security, and compliance control standards. These audits result in audit reports and are conducted: (a) by an

external independent third party; (b) at least annually; (c) in accordance with SOC2 standards or it's alternative standards that are substantially equivalent.

6 Other EA Privacy Provisions

6.1 EA Website

Our website may automatically record some general information about a site visit which EA then uses for statistical analysis to help make the website more useful to visitors. This information might include: Internet domain for the visitor's Internet service provider, such as 'company.com' or 'service.ca'; IP address of the computer accessing the website, type of browser used, such as Mozilla Firefox or Google Chrome; type of operating system used, such as Windows or Macintosh; date and time of the visit to the EA website and web pages that are visited on the EA website; and address of the previous website visited, if the site visitor was linked to EA from another website.

EA also uses "cookies" that identify anyone as a return visitor, and which can help EA tailor information to suit the individual preferences of the visitor. A cookie is a piece of data that a website can send to a visitor's browser, which may then store the cookie on the visitor's hard drive. The goal is to save time and provide the user with a more meaningful visit and to measure website activity. Cookies do not contain any personally identifying information.

Our Privacy Notice at http://www.environicsanalytics.ca/footer/privacy discloses the privacy practices for the EA website. However, the EA website contains links to other sites. Once a visitor links to another site, the visitor is subject to the privacy and security policies of the new site.

6.2 Children's Privacy

EA services do not knowingly collect, use, or disclose personal information from children under the age of 13 or as otherwise identified.

6.3 Consumer Communication with Environics Analytics

Consumers may contact EA, via telephone, email, or other means, and their messages to EA may contain their name and email address along with any other information they may wish to include in the text of their message. EA may keep a record of the correspondence, but EA does not make use of the email address or other contact information unless it is to correspond with the consumer as necessary.

6.4 Canada's Anti-Spam Legislation (CASL) Compliance

CASL came into effect July 1, 2014 and established the framework for what businesses can do when using electronic channels to promote, or market themselves, or their products and services to an electronic address of Canadians (for example via email or text message). The law applies to both Canadian and non-Canadian businesses.

Environics Analytics has a duty to understand and comply with the law. EA must establish an internal compliance regime to ensure that EA Staff who send commercial messages understands and complies with the law.

6.5 Consumer Choice and the CMA/DMA Do Not Contact Lists

One of our most important principles is to let consumers choose to be removed from lists maintained by Environics Analytics for its own purposes. Environics Analytics is a member of the Canadian Marketing Association (CMA) and the Data & Marketing Association and abides by their ethical guidelines. We encourage all our clients to keep an updated list of individuals and businesses who have requested that they do not receive any third-party advertising from them and to register with the CMA's Do Not Contact service, described below.

The Canadian Marketing Association (CMA) maintains a Do Not Contact service that lets individuals reduce the number of marketing offers they receive by mail. Consumers register to have their names removed from

marketing lists held by members of the Canadian Marketing Association and other companies using the service. Consumers can register for the Do Not Contact Service by visiting www.the-cma.org. Similarly, the DMA offers a free service to consumers for Mail and online advertising and can be accessed at https:/thedma.org/resources/consumer-resources.

In addition, Canadian consumers can reduce unwanted telemarketing calls by registering their telephone number with the National Do Not Call List (DNCL). A consumer can register a telephone number for the National Do Not Call Service by visiting www.lnnte-dncl.gc.ca/index-eng. For U.S. citizens, the equivalent service is offered at https://www.donotcall.gov/ where consumers can register up to three telephone numbers at the same time.

Consumers can be removed from our lists by contacting our Privacy Officer as per below:

Email: privacy@environicsanalytics.com
Phone: (647) 800 1498
Mail:
Environics Analytics Privacy Officer
33 Bloor Street East, Suite 400
Toronto, ON M4W 3H1

6.6 Accuracy; Consumer Access to Personal Information

Environics Analytics seeks to ensure that Personal Information we hold for our own purposes, including licensing to outside parties, is accurate, complete, and up to date. We will make all reasonable efforts to make available to consumers any Personal Information about them that is held by it for its own purposes upon a written request from the individual or from their designate holding a power of attorney. If following the review of the Personal Information, they can demonstrate that the Personal Information is inaccurate or incomplete, EA will remove the Personal Information as requested. If they wish to have the data corrected in a directory from which EA obtained it, they must contact their directory owner, as EA cannot do so on their behalf.

In order for EA to accommodate any request, the consumer will be required to provide Environics Analytics with enough information for Environics Analytics to determine if they are present in our files. The information that they provide for this reason will not be used for any other purpose.

EA Privacy Officer will follow a comprehensive process to address the request, which includes documenting a record of the associated activity.

For more information on Consumer Access to Personal Information, or if you (EA Staff) wish to you access or correct your personal information please contact

Environics Analytics Chief Privacy Officer
Email: Privacy@environicsanalytics.com
Phone: 888.339.3304 x1498

Or by Mail

33 Bloor Street East Suite 400
Toronto ON M4W 3H1
Canada

6.7 Ethical Relationships

EA conducts relationships with clients, suppliers, and partners in an ethical and professional manner. EA is a member of both the Data Marketing Association (DMA), now part of the Association of National Advertisers (ANA), and the Canadian Marketing Association (CMA), http://www.the-cma.org, and abide by their ethical guidelines.

It should also be noted that EA is committed to industry self-regulation, and as such, is a member in good standing with the Interactive Advertising Bureau (IAB) and is in compliance with the Digital Advertising Alliance (DAA) Self-regulatory Code.

6.8 How to Contact EA Regarding Privacy

EA has appointed a Chief Privacy Officer (CPO) to ensure accountability, to effectively manage a privacy management program designed to protect privacy, and to set policies and processes. To contact EA regarding complaints, express concerns, or provide feedback regarding EA privacy practices can be done by emailing, phoning, or mailing the Chief Privacy Officer using the information below.

In addition, requests for individual access or any other inquiry regarding our privacy practices, should be sent to the Chief Privacy Officer using the same information below.

EA will respond in a timely manner to your requests.

Environics Analytics Chief Privacy Officer
Email: Privacy@environicsanalytics.com
Phone: 888.339.3304 x1498

Or by Mail

33 Bloor Street East Suite 400
Toronto ON M4W 3H1
Canada

7 Privacy Policy Maintenance

7.1 New Staff

Upon on-boarding new staff, it is required that each new staff print and sign a "receipt and acknowledgment form" which indicates that they have read and understood the policies outlined in the:

a. Privacy Policy
b. EA Employee Guide
c. Master Information and Security Policies

The "receipt and acknowledgment form" is stored within the Environics Analytics Human Resources and Administration dept. for the new staff.

7.2 Process for Changes

- Privacy Policy changes to existing policies are to be submitted, via email, from Environics Analytics employees to a member of the Compliance Office. Alternatively, a member of the Compliance Office and/or EASMT can forward a change request to the Compliance Office
- A member of the Compliance Office will review the proposed policy and/or policy change. The Compliance Office will present a concise statement outlining the proposed policy, or policy change, and its implications, to the remaining members of the EASMT at the next Compliance Office Meeting
- Stakeholders, within the EASMT, will review and/or respond to the proposal
- The Compliance Office will issue an approval decision on the proposed policy or change. The initiator of the policy or change process will be informed as to the decision
- For accepted new policies and/or changes, this document will be revised and re-published, incorporating the policy or change

7.3 Review

The Internal EA Privacy Policy will be reviewed every 12 months from the last revision date by the Privacy Officer.

7.4 Revision History

All changes to the Environics Analytics Privacy Policy will be documented in the Revision History Summary.