EMPLOYEE PRIVACY POLICY

1. POLICY OVERVIEW

1.1 PURPOSE

Corus Entertainment Inc. and its affiliates ("**Corus**", "**we**" or "**us**") are committed to transparency, accountability and security with respect to the collection, use, disclosure and storage of the Personal Information of Corus employees (collectively, the "**Employees**" or "**you**"). We strictly follow the guidelines outlined in Canada's *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) (see https://laws-lois.justice.gc.ca/eng/acts/P-8.6/).

The purpose of this policy (the "**Policy**") is to help you understand how and why we handle your Personal Information, specifically:

1.2 SCOPE

This Policy applies to all Corus Employees, subject to any exceptions that we inform you with respect to the location in which you are based. Employees must review and accept the terms of this Policy as a condition of forming and maintaining an employment relationship with Corus. You must act in strict compliance with this Policy at all times when and if you handle the Personal Information of other Employees, including after you cease to be an Employee.

2. POLICY OWNER

Corus' People Team and Privacy Officer are the joint custodians of this Policy. If you have any questions or concerns about this Policy, please do not hesitate to contact your People Team representative or our Privacy Officer at privacy@corusent.com.

3. WHAT IS PERSONAL INFORMATION?

3.1 "**Personal Information**" means information about an identifiable individual. "Identifiable individual" means that there is a serious possibility that an individual could be identified through the use of the information, alone or in combination with other information.

3.2 For the purposes of this Policy, Personal Information does not include your name, title, business address or business telephone number, to the extent it is collected, used or disclosed by us for the purpose of communicating or facilitating communication with you in relation to your employment with Corus.Elec

4. WHAT PERSONAL INFORMATION DO WE COLLECT ABOUT YOU?

4.1 During the course of your employment with Corus, we may collect various kinds of Personal Information from or about you, including the Personal Information set out in Appendix 1.

5. WHY DO WE COLLECT, USE AND DISCLOSE YOUR PERSONAL INFORMATION?

5.1 We collect, use and disclose your Personal Information in order to establish, manage or end our employment relationship with you and for limited other purposes prescribed by law, including the activities and purposes set out in Appendix 2.

5.2 We will seek your consent to collect, use or disclose your Personal Information for any purpose other than those set out in Section 5.1 above. We may ask you to express your consent in several ways, such as verbally, in writing or electronically. You may withdraw your consent at any time after it is provided by contacting your supervisor or People Team representative.

6. HOW DO WE STORE YOUR PERSONAL INFORMATION?

6.1 Most of the Employee Personal Information that we collect is stored electronically on local servers administered by us, or external servers administered by our service providers. The external servers are generally located within Canada, but in some cases may be located in the United States or other countries. We are required to maintain certain Personal Information in hard copy form on our premises.

6.2 We store Employee Personal Information for as long as reasonably necessary to fulfill the purpose of collection, or such longer period specified by law.

6.3 We are accountable for safeguarding the Employee Personal Information that we collect, use and disclose from loss, theft, and unauthorized access, disclosure, modification or duplication. We accordingly employ various technological, physical and organizational safeguards to ensure the security and integrity of the Personal Information. Examples include locked filing cabinets, restricted access to offices, file access rights, and electronic security measures such as passwords, PIN numbers and encryption. These safeguards are reviewed on an ongoing basis to ensure security is maintained.

7. WHO ACCESSES AND PROCESSES YOUR PERSONAL INFORMATION?

7.1 Our Employee Personal Information is primarily processed by our People Team and by appropriate Corus management staff.

7.2 In some instances, we engage third parties to process Employee Personal Information on our behalf. We oblige such third parties contractually to process Personal Information on our instructions and to take steps to ensure that Employee Personal Information remains protected. While the specific third party processors change from time to time, the categories of third party processors are set out in Appendix 3.

8. HOW CAN YOU ACCESS AND UPDATE YOUR PERSONAL INFORMATION?

8.1 We take appropriate measures to ensure that the Personal Information we hold about you is accurate, complete and, where necessary, up to date. However, it is also your responsibility to ensure that your Personal Information is kept as accurate, complete and current as possible. In many cases, you will be able to update your Personal Information through the self-service function of Corus' automated human resource management systems. Please inform your supervisor or People Team representative if there are any changes or errors in your Personal Information that you cannot update by yourself, or that you need assistance to update.

8.2 Upon request, we will inform you of the existence, use and disclosure of your Personal Information and give you access to that information. You will be able to challenge the accuracy and completeness of the information and have it amended as appropriate. Access to and amendment of your Personal Information will be made within a reasonable timeframe. There are certain circumstances provided by law in which we must or may refuse access to your Personal Information, as described in Appendix 4.

9. HOW DOES CORUS USE ELECTRONIC MONITORING?

9.1 In this section we describe Corus' approach to electronic monitoring. Electronic monitoring may be used to collect information about employee activities in the workplace or when employees work remotely.

9.2 "electronic monitoring" includes all forms of employee and assignment employee monitoring that is done electronically.

9.3 Corus conducts continuous electronic monitoring on Corus' IT systems, devices, and premises, and uses information gathered from that monitoring, as follows:

- Network Access
    - Monitoring: Your access to Corus' computers, networks, programs and files, work email communications, internet browsing ("IT systems") is logged to record the identity of the accessor, the resources accessed, and changes made to IT systems.
    - Purpose: Security of IT systems and employer confidential information. Monitoring ensures that there is no unauthorized access of Personal Information or corporate data internally or externally. Further, monitoring ensures that only approved devices join our network, that they are up to date. It also assists with Corus asset management and to minimize asset loss. Additionally, monitoring aids in verifying whether employees are either working from Corus premises or remotely when using Corus-issued devices, and this data is only available upon authorized request. Finally, it assists with the identification of instances of potential violations to the Corus Code of Conduct or internal policies, which are then reviewed further.
- Corporate Mobile Devices and personal devices used to access Corus systems
    - Monitoring: Your access to Corus issued laptops, mobile phones and tablets are logged with multiple security tools to manage devices and secure organizational data that an employee may access or use on their devices.
    - Purpose: Security of IT systems and employer confidential information. Monitoring ensures that only approved devices join our network, that they are up to date, and do not become infected with any type of malware or viruses. It also assists with Corus asset management and to minimize asset loss. Additionally, monitoring aids in verifying whether employees are either working from Corus premises or remotely when using Corus-issued devices, and this data is only available upon authorized request. Finally, it assists with the identification of instances of potential violations to the Corus Code of Conduct or internal policies, which are then reviewed further.
- Corus Premises
    - Monitoring: Use of video camera to monitor or capture visual images of activities on Corus premises. Video monitoring does not capture audio.
    - Purpose: Used on applicable Corus premises to ensure that employees, visitors, and Corus assets are safe from theft, vandalism, or other form of misconduct.

9.4 Any personal information about you collected through electronic monitoring will be collected, used and disclosed only for the purposes described in this section, and will be subject to security, retention and access as described in this Policy.

9.5 Corus will maintain and revise this section as required to ensure it reflects current monitoring practices.

10. HOW DO YOU REPORT AN ACTUAL OR POTENTIAL LOSS, WRONGFUL ACCESS OR MISUSE OF EMPLOYEE PERSONAL INFORMATION?

10.1 The safety and security of our Employees' Personal Information is paramount. If you believe that there has been an actual or potential loss, wrongful access or misuse of Employee Personal Information, **please immediately contact the People Team at** people@corusent.com **or Corus' Privacy Officer at** privacy@corusent.com. If you prefer to remain anonymous, please call the Corus Alert Line 24/7 at **1-800-750-4972.** If you call this hotline and choose to remain anonymous, you will not be asked to identify yourself and your phone number will not be reported or recorded. The Corus Alert Line is operated by a third party service provider that specializes in confidential intake and reporting – you will not be speaking to a Corus operator.

10.2 We emphasize that it is imperative that you report the actual or potential problem immediately. This allows us to contain any damage or loss, inform affected individuals as appropriate, and take steps to limit or eliminate any risk of harm to affected individuals.

10.3 We will notify you if there is a data breach involving your Personal Information that gives rise to a real risk of significant harm. We will also advise what steps we are taking to contain and mitigate the harm.

DATE OF REVIEW / UPDATE	COMMENTS	APPROVED BY
January 15, 2020	Policy revised and updated	Peter Morley, VP, Associate General Counsel, Corporate
January 29, 2020	Formatting Changes	Peter Morley, VP, Associate General Counsel, Corporate
October 11, 2022	Introduction of Section 9 – Employee Electronic Monitoring	Brad Chapman VP, Associate General Counsel, Corporate Matt Thompson VP, Associate General Counsel, Chief Privacy Officer

APPENDIX 1

Types of Personal Information We May Collect

1) Name;
2) Gender;
3) Date of birth;
4) Next of kin, dependents and beneficiaries;
5) Marital status;
6) Contact information such as home address, telephone number, email address and emergency contact names and their contact information;
7) Past employment details, social insurance or other national insurance or other government issued identification information, including driver's license information;
8) Information and documentation required under immigration laws such as passports, work permits, citizenship and residency information;
9) Family data and health-related information in order to provide applicable benefits;
10) Pay and financial information for payroll, taxes, expense reimbursement and related purposes, including base salary, bonus, benefits, incentive compensation, and bank information;
11) Information necessary to evaluate performance, including salary reviews, disciplinary records, talent reviews and performance appraisals;
12) Management records such as working time records, vacation/holiday and other paid time off or absence records;
13) Social media activity;
14) System access information such as system ID, email account and system passwords; and
15) Employment equity data.

APPENDIX 2

Potential Uses of Employee Personal Information

1) Perform recruitment;
2) Administer benefits, including medical, pension and other benefits, and eligibility of dependents;
3) Administer salary and expenses, payment administration, reviews, wages, and other awards such as bonuses, commissions and incentive plans;
4) Carry out performance appraisals, career planning, training, promotions, transfers and skills monitoring; managing sickness or other types of leave;
5) Honour other contractual employment benefits;
6) Provide employee references;
7) Perform workforce analysis and planning;
8) Perform employee surveys;
9) Perform background checks, employment reference checks, credit checks and education verifications;
10) Manage disciplinary matters, grievances and terminations;
11) Review employment decisions;
12) Make business travel arrangements;
13) Manage business expenses and reimbursements;
14) Plan and monitor training requirements and career development activities and skills;
15) Create and maintain internal employee directories and internal alerts regarding birthdays and service anniversaries;
16) Administer income tax and other deductions;
17) Comply with record-keeping and reporting obligations at law;
18) Comply with government or regulatory inspections, audits and other requests (including to meet national security or law enforcement requirements);
19) Respond to legal process such as subpoenas or garnishments;
20) Create and administer emergency response and communication plans;
21) Contact designated individuals in the event of a workplace accident or emergency.
22) As necessary to enable Corus to protect its legitimate interests, pursue legal rights or remedies (for instance, when necessary to prevent or detect fraud or crime), defend litigation and manage internal complaints or claims;
23) Conduct internal investigations/audits and comply with internal policies;
24) Garnishments;
25) Electronic monitoring of Corus systems that an employee may access or use on their devices.
26) Evaluate and/or complete a business transaction such as mergers and acquisitions; and
27) Such other purposes permitted or required by law.

APPENDIX 3

Third Party Service Providers

1) Human resource system providers;
2) Payroll administration providers;
3) Pension and benefits consultants and administrators;
4) Benefit providers, such as Employee discount programs;
5) Insurance providers and brokers;
6) Employee engagement service providers;
7) Investment plan administrators; and
8) Such other categories of third parties as are reasonably necessary to administer the employment relationship and fulfill the purposes set out in this Policy.

APPENDIX 4

Denial of Access to Personal Information

1) We must refuse to provide you access to your Personal Information:

   (a) if it would reveal Personal Information about another individual*, unless there is consent or because an individual's life, health or security is threatened; or

   (b) if we have disclosed your Personal Information to a government institution for law enforcement or national security reasons. Upon request, the government institution may instruct us to refuse access or not to reveal that the Personal Information has been disclosed by us. In such cases, we must refuse the request and notify the Privacy Commissioner of Canada. We are not permitted to inform the individual of the disclosure to the government institution, or that the institution was notified of the request, or that the Commissioner was notified of the refusal.

2) Corus may refuse access to personal information if the information falls under one of the following:

   (a) solicitor-client privilege;

   (b) confidential commercial information*;

   (c) disclosure could harm an individual's life or security*;

   (d) it was collected without the individual's knowledge or consent to ensure its availability and accuracy, and the collection was required to investigate a breach of an agreement or contravention of a federal or provincial law (the Privacy Commissioner of Canada must be notified);

   (e) It was generated in the course of a formal dispute resolution process;

**If these details can be removed from any requested documentation, Corus must then release the remaining information in the document.*