

Standard for Privacy of Personal Information

Accountable Owner:	Alan O'Brien, Sr VP – General Counsel and Secretary	Responsible Author:	Josh Share, VP – Human Resources				
Publish Date:	22-Mar-18	Required Review Frequency:	22-Mar-21				
Effective Date:	31-Mar-18	Revision:	2.0				
Policy Statement Number: <i>Refer to NMS Policy Framework</i>	11.1	Asset Life Cycle: <i>Mark the box(es) that are applicable to this Standard.</i>	Explore	Develop	Produce	Market	Abandon
			X	X	X	X	X

CONTENTS

1.0 INTRODUCTION TO THIS STANDARD 2

2.0 REQUIREMENTS OF THIS STANDARD..... 3

3.0 REFERENCES AND RELATED INFORMATION..... 4

APPENDIX A: RESPONSIBILITIES 5

APPENDIX B: PROCEDURE FOR ACCESS TO PERSONAL INFORMATION..... 6

APPENDIX C: REQUEST FOR ACCESS TO PERSONAL INFORMATION FORM..... 7

APPENDIX D: EMPLOYEE CONSENT FORM..... 8

APPENDIX E: PROCEDURE TO CHALLENGE THE COMPANY’S COMPLIANCE WITH APPLICABLE PRIVACY LEGISLATION.....12

APPENDIX F: PRIVACY OF PERSONAL INFORMATION BREACH RESPONSE PLAN13

For Revision and Approval history, see Nexen Management System approval workflow.

1.0 INTRODUCTION TO THIS STANDARD

1.1 PURPOSE

The purpose of this Standard is to establish procedures for ensuring that the Company complies with the *Personal Information Protection Act* (“PIPA”) and Canada’s *Personal Information Protection and Electronic Documents Act* (“PIPEDA”) and any other applicable legislation (collectively, the “Applicable Privacy Legislation”) when collecting, using, disclosing and retaining Personal Information in the course of business by the Company.

1.2 SCOPE

This Standard applies to all areas of the Company’s business.

1.3 PERSONS AFFECTED

Role	Description
All Directors, officers, Employees and Contingent Workers of the Company and any other party acting on the Company’s behalf.	<ul style="list-style-type: none">Will adhere to the requirements in this Standard.

1.4 DEFINITIONS OF TERMS

Capitalized terms used in this Standard have the meanings set out in the [Nexen Glossary](#).

1.5 QUESTIONS

Questions regarding this Standard should be directed to the Privacy Officer.

If concerns regarding the handling of Personal Information or requests for access to Personal Information arise and further discussion with the Company is desired, individuals should address any such concerns or requests, in writing, to the Privacy Officer, the individual appointed as responsible for the Company’s compliance with the Applicable Privacy Legislation and the Company’s Standard.

Privacy Officer: Chuck (Marianne) Davies

Address: 801 – 7th Ave. SW

Calgary, Alberta T2P 3P7

2.0 REQUIREMENTS OF THIS STANDARD

The following table outlines the minimum requirements and quality expectations that must be satisfied to meet the intent of this Standard.

2.1 STANDARD REQUIREMENT TABLE

Requirement Number	Employee, Contingent Worker and Contractor Requirements
2.1.1	<p>In all instances where personal information is collected, used and disclosed, must follow Schedule 1 of PIPEDA, Part 1 in order to honour the intent of “Privacy of Personal Information”.</p> <p>This schedule lists the ten principles of fair information practices that form the rules for the collection, use, disclosure and retention of Personal Information and which give individuals control over how their Personal Information is collected, used and disclosed. Refer to Appendix A: Responsibilities for the ten principles of fair information practices.</p>
2.1.2	<p>Unless permitted by law, an individual’s (Employee, Contingent Worker, Contractor or customer) consent must be obtained when collecting, using or disclosing individual’s Personal Information. Information collected is to be restricted to only information actually required. New Employee forms or changes to Employee forms intended to gather information must be reviewed by the Company’s Privacy Officer.</p>
2.1.3	<p>Must use Personal Information only for purposes for which it was collected.</p> <p>If needed for another purpose, specific consent for the incremental purpose must be obtained.</p>
2.1.4	<p>Personal Information must be kept current and accurate.</p> <p>It is the responsibility of each Employee, Contingent Worker and Contractor to keep his or her Personal Information pertaining to home addresses, dependents, beneficiaries, or anything else that may affect that Employee’s or Contingent Worker’s benefit status current.</p>
2.1.5	<p>Personal Information must be protected by specific safeguards, as required in the circumstances (e.g. locks, passwords, and encryption).</p> <p>Employees, Contingent Workers and Contractors are expected to make use of protection tools such as locks, passwords and encryption to protect all Personal Information in the Company’s control. When no longer required, Personal Information will be made anonymous or destroyed in accordance with the appropriate Records Classification and Retention Schedule.</p>
2.1.6	<p>Must follow the Procedure to Access Personal Information (Refer to Appendix B) in order to either access one’s own Personal Information held by the Company or to challenge its accuracy.</p>
2.1.7	<p>If an individual wishes to challenge the Company’s compliance with the principle of the Applicable Privacy Legislation, must follow the Procedure to Challenge the Company’s Compliance with the Applicable Privacy Legislation. See Appendix E.</p>

2.2 MEASURING CONFORMANCE AND CONTINUOUS IMPROVEMENT

The following table summarizes the methods that must be used to measure conformance with the intent of this Standard.

Method of Measurement	Means of Verification	Role for Review and Interval	Location of Key Records and Reports
Standard review and update (if applicable)	Self-Assessment	Responsible Author – as defined by Accountable Owner Interval: 3 years	Legal Standards

The Method of Measurement, identified above, will be used as a foundation to determine whether this Standard is effective and efficient; and, whether opportunities exist to improve further. Refer to the [NMS Assurance Activities Business Process](#) for further details.

Audit requirements of this Standard will be determined by the Nexen’s Corporate Audit group in conjunction with the Legal Department.

3.0 REFERENCES AND RELATED INFORMATION

3.1 EXTERNAL REFERENCES

Personal Information Protection Act, SA 2003, c P-6.5

Personal Information Protection and Electronic Documents Act, SC 2000, c 5

3.2 INTERNAL REFERENCES

Not Applicable

3.3 RELATED INFORMATION

Not Applicable

APPENDIX A: RESPONSIBILITIES

In order to honour the intent of “Privacy of Personal Information”, the Company follows Schedule 1 of the PIPEDA, Part 1. This schedule lists the ten principles of fair information practices that form the rules for the collection, use, disclosure and retention of Personal Information and which give individuals control over how their Personal Information is collected, used and disclosed.

The ten principles are:

1. **Accountability:** The Company is responsible for Personal Information under its control and will designate an individual responsible for the Company’s compliance with Applicable Privacy Legislation.
2. **Identify purposes:** Before or as Personal Information is collected, the Company will identify and advise the individual why it is needed and how it will be used or disclosed.
3. **Consent:** The knowledge and consent of the individual are required for the collection, use or disclosure of Personal Information, with a few exceptions.
4. **Limit collection:** The Company will not collect Personal Information indiscriminately and will avoid actions that may mislead individuals about reasons for collecting Personal Information.
5. **Limit use, disclosure and retention:** Personal Information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal Information will be retained only as long as necessary for fulfillment of those purposes in accordance with Records Management policies.
6. **Accuracy:** Personal Information will be as accurate, complete and current as necessary.
7. **Safeguards:** Personal Information will be protected against loss, theft, unauthorized access, disclosure, copying, use or modification regardless of the format in which it is held.
8. **Openness:** The Company will make available to individuals specific information about its policies and practices related to management of Personal Information.
9. **Individual Access:** When requested in writing, the Company will allow an individual, with some exceptions, access to his or her own Personal Information and advise the individual how the information has been used and to whom it has been disclosed. The individual may correct or amend any Personal Information if accuracy and completeness is challenged and found deficient.
10. **Provide Recourse:** An individual may address a challenge concerning compliance with the above-noted principles to the individual accountable for the Company’s compliance (Privacy Officer).

APPENDIX B: PROCEDURE FOR ACCESS TO PERSONAL INFORMATION

1. Address, in writing, a request to the Privacy Officer to access your Personal Information. See Appendix C for Request to Access to Personal Information Form
2. The Company will respond to the request within 30 days (with a possible 30-day extension) at minimal or no cost to the individual.
3. The Company will advise if the release of the Personal Information requested is prohibited due to a legal reason or a conflict with another individual's protection of Personal Information.
4. Having reviewed his or her Personal Information, if an individual demonstrates the inaccuracy or incompleteness of the Personal Information, the Company will amend the Personal Information as required.
5. If requested, the individual will be advised as to the names of third parties having received, or likely to have received, this Personal Information and amendments will be forwarded to these third parties.
6. If an individual has reviewed his or her Personal Information in accordance with 4 above and, based on a review of the individual's request, the Company finds there is no inaccuracy or incompleteness and chooses not to amend the Personal Information, the Company will keep a record of this decision including the reasons therefor on the Company's records.

APPENDIX C: REQUEST FOR ACCESS TO PERSONAL INFORMATION FORM

Individual's Name: _____

Employee Number (if applicable): _____

Address: _____

Telephone Number: _____

Company Connection: _____

(Please state your current or past relationship with the Company i.e. employee, former employee, customer, contractor, consultant, vendor, et cetera)

Requested Period: _____

(Please state the date(s) of the period of personal information requested.)

Direct Contact or
Supervisor: _____

Location of Employment/
Service: _____

Signature: _____

PLEASE COMPLETE THE ABOVE INFORMATION REQUEST AND SUBMIT IT TO THE NEXEN ENERGY ULC PRIVACY OFFICER. THE INFORMATION PROVIDED HEREIN WILL BE USED ONLY TO LOCATE AND IDENTIFY THE INFORMATION REQUESTED BY YOU AND WILL BE COMMUNICATED TO YOU AT MINIMAL OR NO COST. YOUR SIGNATURE ABOVE INDICATES CONSENT FOR USE OF THE PERSONAL INFORMATION PROVIDED IN ORDER TO LOCATE AND ACCESS PERSONAL INFORMATION UNDER THE CONTROL OF NEXEN ENERGY ULC.

APPENDIX D: EMPLOYEE CONSENT FORM

The purpose of this document is to give my consent to Nexen¹ to collect, use and disclose my Personal Information in accordance with Nexen's *Standard for Privacy of Personal Information* and privacy practices and to agree to abide by Nexen's privacy Standard and practices.

Definitions

For purposes of this document, the following definitions apply:

“*Employee*” includes an individual seeking to be employed, currently employed or formerly employed by Nexen.

“*Employee Personal Information*” means, in respect of an individual who is an Employee, personal information reasonably required by an organization that is collected, used or disclosed solely for the purposes of establishing, managing or terminating the employment relationship.

“*Personal Information*” means information about an identifiable individual.

Types of Information Collected

Nexen collects and maintains different types of Personal Information from Employees, including:

- (a) Identification information such as an Employee’s name, home address, telephone, personal e-mail address, date of birth, social insurance number, marital and dependent status and photo;
- (b) Employment information such as an employee’s job title, resumes, letters of offer and acceptance of employment, compensation and benefit information, background verification information, drivers' abstracts, employment references, emergency contact information, emergency identification for international travel and evaluations;
- (c) Information required by Government officials in foreign jurisdictions for purposes of VISA's, work permits or such similar business requirements;
- (d) Benefit information such as forms relating to the application or change of employee health and welfare benefits, including but not limited to health care, life insurance, short and long term disability, medical and dental care, savings plan, pension plan;
- (e) Financial information such as bank account numbers and tax related information;
- (f) Fitness to work information such as pre-employment medicals, annual medicals and audiometric examinations; and
- (g) Other information necessary for Nexen's business purposes, which may be voluntarily disclosed or collected in the course of an individual’s application to and employment with Nexen.

Collection Sources

Nexen collects Personal Information through a variety of means and from different sources, including but not limited to Personal Information that:

- (a) Employees provide in conversations, in correspondence or through applications and other forms;

¹ In this document, “Nexen” refers to Nexen Energy ULC and its majority owned subsidiaries and affiliates for which it has managerial responsibility.

- (b) Nexen receives from third parties, such as individuals or organizations who provide test results, temporary and permanent placement services, administration of benefits and pensions, drivers abstracts, pre-employment medical results and references;
- (c) Employees provide using Nexen's office and computer equipment and software, including e-mail and Internet applications; and,
- (d) Employment evaluations and investigations which are reasonably required to manage the employment relationship.

Nexen uses the information provided verbally or in writing by individuals upon their application for employment (and/or which may be provided during the course of employment by Nexen), for different purposes in the management and administration of the employment relationship between Nexen and that individual.

Use of Information

The purpose for the use (as well as the initial collection and possible disclosure) of Personal Information is for the administration, planning and management of an individual's employment relationship with Nexen and includes, but is not limited to:

- (a) Initial employment, including the verification of references and qualifications;
- (b) Administering compensation and benefits;
- (c) Processing of employee work-related claims (e.g., worker compensation, insurance claims, short term and long term disability claims, etc.);
- (d) Performance and training requirements;
- (e) Assessing qualifications for a particular job or task;
- (f) Gathering evidence for corrective action, should it be necessary;
- (g) Establishing a point of contact in the case of an emergency;
- (h) Compiling directories for work related purposes;
- (i) Compiling information for use in making travel arrangements;
- (j) Compiling information in order to plan social activities;
- (k) Compiling photos of employees for use on building access cards, internal directory and internal and external publications published by Nexen;
- (l) Compiling information for ergonomic assessments;
- (m) Complying with applicable labour or employment statutes;
- (n) Ensuring the security of company-held information; and
- (o) For such other purposes as is required for administration of the employment relationship by Nexen.

Nexen does not sell, trade, barter or exchange for consideration Personal Information about any Employee.

There are circumstances where the use and/or disclosure of Personal Information may be justified or permitted or where Nexen is obliged to disclose information without consent. Such circumstances may include:

- (a) Where required by law or by order of a court, administrative agency or other governmental tribunal;

- (b) Where Nexen believes, upon reasonable grounds, that it is necessary to protect the rights, privacy, safety or property of an identifiable person or group;
- (c) Where required, to determine or administer Employee pay and benefits;
- (d) Where it is alleged that the person concerned or Nexen may be guilty of a legal offence; civilly liable in a legal action;
- (e) Where an investigation is required for breach of company policies or job standards;
- (f) Where the information is part of downsizing and/or job elimination;
- (g) Where it is necessary to permit Nexen to pursue available remedies or limit any damages that it may sustain; and
- (h) Where the information is public.

Where obliged or permitted to disclose information without consent, Nexen will not disclose more information than is required.

Nexen may disclose Personal Information of Employees to organizations that assist Nexen by performing services on its behalf (i.e., benefits and pension administrator, payroll administrator, temporary and permanent staffing agencies, employee and family assistance program providers, employee medicals). Personal Information will only be provided to such organizations if they agree to use such information solely for the purposes of providing services to Nexen and under the instruction of Nexen and, with respect to that information, to act in a manner consistent with the relevant principles articulated in Nexen's Privacy Policy. In an event of a change in suppliers, your Personal Information may be passed to a new supplier.

Personal Information may also be subject to transfer to another company in the event of a change of ownership of all or part of Nexen or any of its subsidiaries. This will occur only if the parties have entered into an agreement under which the collection, use and disclosure of the information is restricted to those purposes that relate to the business transaction, including a determination whether or not to proceed with the business transaction, and is to be used by the parties to carry out and complete the business transaction.

All employment files are securely maintained in the Human Resources office of Nexen's Calgary office. Nexen shares Personal Information contained within the employment files only with those staff members of Nexen who need it to ensure that Employees are properly compensated, or those who are involved in the hiring, supervision, promotion, discipline or termination of Employees. Personal information in document form is kept in secure locked offices, and computer information is maintained in secure files with limited access.

Nexen will engage service providers outside Canada, specifically in the United States, China and the United Kingdom, to process Personal Information for the purpose of business management. If you wish to access written information about Nexen's policies and practices regarding service providers outside Canada, please consult the Nexen *Standard for Privacy of Personal Information*. If you have any questions about the collection, use, disclosure of Personal Information by a service provider outside Canada, please contact the Company's Privacy Officer.

Monitoring

During the term of your employment with Nexen, your access to Nexen facilities may be tracked for security purposes and your use of the internet and e-mail via the Nexen network may be monitored to ensure compliance with Nexen Standards governing internet access and e-mail usage. (See *Standard for IT Acceptable Use*)

Retention

Nexen retains Personal Information about Employees as long as Nexen believes it is necessary to fulfill the purpose for which it was collected. Nexen has in place a Records Management Policy and Records Retention Schedule that outlines the procedures for the retention and subsequent disposition of Nexen records including those that contain Personal Information.

Security

Nexen endeavors to maintain adequate physical, procedural and technical security with respect to its offices and information storage facilities so as to prevent any loss, misuse, unauthorized access, disclosure, or modification of an Employee's Personal Information.

As part of those precautions, Nexen restricts access to an Employee's Personal Information to those Employees and others (i.e., individuals or organizations providing services to Nexen) that it determines need to know that information in order that Nexen may conduct its activities.

If any Employee misuses the Personal Information of another Employee, this will be considered a serious offence for which appropriate disciplinary action may be taken, up to and including termination of employment. If any individual or organization misuses the Personal Information of an Employee, which was provided solely for the purpose of providing services to Nexen, this will be considered a serious issue for which appropriate action may be taken, up to and including termination of the service agreement.

CONSENT

I acknowledge that I have read and agree to abide by Nexen's *Standard for Privacy of Personal Information*.

I consent to Nexen collecting, holding, receiving, storing, accessing, using, disclosing, processing or transferring my Personal Information, in electronic or any other form, for the purposes and to parties described above. This consent covers the period of my employment with Nexen and for such time as may be required for business purposes after the end of employment with Nexen.

I understand that Nexen has undertaken the responsibilities under the *Personal Information Protection Act*, the *Personal Information Protection and Electronic Documents Act*, and other applicable legislation, to protect my Personal Information from misuse, or unauthorized disclosure.

I understand, to the extent possible in my employment relationship with Nexen, that I may, at any time, withdraw the consent hereby given by notifying Nexen in writing of such withdrawal. I further understand that any such withdrawal of consent may affect certain aspects of my employment relationship or result in me being no longer eligible for certain employment benefits and services provided to me by Nexen and/or the third parties selected by Nexen to render such services, to the extent the Personal Information affected by the withdrawal of my consent was necessary to process such benefits. I also understand that if I do not consent to, or if I withdraw consent to the collection, use, retention, and disclosure of certain Personal Information then Nexen may not be able to employ or continue to employ me.

Employee Signature

Employee Name (print)

Date

APPENDIX E: PROCEDURE TO CHALLENGE THE COMPANY'S COMPLIANCE WITH APPLICABLE PRIVACY LEGISLATION

1. Address in writing a complaint to the Privacy Officer describing the challenge.
2. Advise Employee, Contingent Worker or Contractor of regulatory agencies that would also handle complaints (if any).
3. The Company will investigate all complaints.
4. If complaint is justified, appropriate measures will be taken.
5. If the complaint believes any resulting action, or inaction, on behalf of the Company in response to the challenge is not in compliance with applicable privacy legislation, the individual will be advised of methods of further recourse.
6. A Breach Response Plan is attached as Appendix F to this Standard.

APPENDIX F: PRIVACY OF PERSONAL INFORMATION BREACH RESPONSE PLAN

Purpose of Plan

The purpose of the Breach Response Plan is to provide a coordinated response to minimize commercial or reputation damage to the Company, its employees or contractors in the event of a Breach of the Privacy of Personal Information Standard. It outlines the procedures to be undertaken in the containment of the Breach and the subsequent actions such as communication, investigation and remediation.

Plan Usage

This Plan is established as a supplement to the Standard for Privacy of Personal Information. It will be activated by the Company's Privacy Officer in the event of a Breach.

Breach Response Team

Name	Contact Numbers	Responsibilities
Alan O'Brien, Sr VP – General Counsel and Secretary	(403) 699-6199	Senior Executive Communication
Tom McNerney, Legal Counsel or designate	(403) 699-5312	Legal Review
Dayna Lee, Manager, Corporate Audit	(403) 699-5191	Audit Investigation
Brittney Price, Manager, Corporate Communications	(403) 699-5585	Communication
Chuck (Marianne) Davies, Privacy Officer	(403) 699-4530	Initial Communication with Team and Privacy Commission/Governing Body
Lynne Steeves, Sr Manager, Total Rewards & HR Operations	(403) 471-6078	Human Resources

Steps to be Undertaken

- ✓ Evaluate the scope of the breach and take steps to contain damage
- ✓ Communicate to Management
- ✓ Address situation with media if required (Tell it All, Tell it Fast, Tell the Truth)
- ✓ Conduct an internal investigation into the matter, report on findings
- ✓ Try to resolve a complainant's concerns informally and early
- ✓ Communicate with the Legislative authorities
- ✓ Notify individuals whose Personal Information has been disclosed
- ✓ Document findings
- ✓ Document and implement remedial actions where appropriate

- ✓ Advise all stakeholders as to the action and remedial action undertaken
- ✓ Address the situation on a systemic basis (company-wide), assess policies/ procedures/staff training.

Incident Tracking

DETAILS OF BREACH

1. Date and Time of Initial Report of Breach: _____
2. Division: _____
3. Location: _____
4. Reporting Individual: (CONFIDENTIAL) _____
5. Date of Breach: _____
6. Time of Breach: _____
7. Description of Breach: _____

