CNOOC International Limited

Standard for Privacy of Personal Information

Conformance with this Standard is mandatory.
You may not 'opt-out' of any requirement identified herein.

Accountable Owner:	**Alan O'Brien**, Chief Legal Officer – CNOOC International	**Responsible Author:**	**Bev Mulder,** VP – HR, Business Partners & Interim VP – HR, Corporate Services					
Publish Date:	21-May-19	**Required Review Frequency:**	21-May-22					
Effective Date:	21-May-19	**Revision:**	5.0					
Policy Statement Number:	12.1	**Asset Life Cycle:**	**Explore**	**Develop**	**Produce**	**Market**	**Abandon**
			X	**X**	**X**	**X**	**X**

CONTENTS

For document history, see the CNOOC International Management System (CIMS).

1.0 INTRODUCTION TO THIS STANDARD

1.1 PURPOSE

The purpose of this Standard is to establish procedures to protect Personal Information collected, Processed or used by the Company and to take steps to ensure that the Company complies with all applicable legislation that establishes rules for the management of Personal Information controlled by organizations, including the *General Data Protection Regulation* ("GDPR"), the *Personal Information Protection Act*s of Alberta and British Columbia, Canada's *Personal Information Protection and Electronic Documents Act* (collectively, the "Applicable Privacy Legislation") when collecting, using, disclosing and retaining Personal Information in the course of business by the Company.

Where there is a conflict between Applicable Privacy Legislation and a requirement of this Standard or the Company's practices, the higher standard will apply.

1.2 SCOPE

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

1.3 PERSONS AFFECTED

Role	Description
All Directors, Employees, Contingent Workers, and officers, of the Company and any other party acting on the Company's behalf.	• Will adhere to the requirements in this Standard.

1.4 DEFINITIONS OF TERMS

Capitalized terms used in this Standard, but not otherwise defined herein, have the meanings set out in the Glossary.

1.5 QUESTIONS

Where a conflict arises with the requirements set out in this Standard, and a Variance is required, refer to Requesting a Variance to CIMS Documents Procedure.

For questions regarding this Standard, concerns regarding the handling of Personal Information, or requests for access to Personal Information, individuals can address any such questions, concerns or requests, in writing, to the Privacy Officer.

Privacy Officer: Robbie Armfield

Address: Suite 2300, 500 Centre St. S.E.

Calgary, AB, Canada T2G 1A6

2.0 REQUIREMENTS OF THIS STANDARD

The following table outlines the minimum requirements that must be satisfied to comply with this Standard.

2.1 STANDARD REQUIREMENT TABLE

Requirement Number	Requirements
Requirements for Directors, Employees and Contingent Workers, and Officers of the Company	
2.1.1	Must follow Applicable Privacy Legislation in all instances where Personal Information is collected, Processed, used or disclosed. The GDPR applies where Personal Information is collected or Processed within the European Economic Area ("EEA") and where Personal Information for Data Subjects resident within the EEA is being collected or Processed outside of the geographical limits of the EEA. Must, in all instances where Personal Information is collected, Processed, used or disclosed and to the extent practicable and where not inconsistent with Applicable Privacy Legislation, follow Schedule 1 of Canada's *Personal Information Protection and Electronic Documents Act*, Part 1, available on the Government of Canada, Justice Laws Website. Failure to comply with this Standard may be grounds for discipline up to and including, but not limited to, termination of employment for cause and may also result in sanctions from applicable authorities at both a Company and a personal level.
2.1.2	Unless permitted by law, a Data Subject's explicit consent must be obtained when collecting, Processing, using or disclosing the Data Subject's Personal Information. Personal Information collected must be restricted to only information actually required. New Employee forms or changes to Employee forms intended to gather information must be reviewed by the Privacy Officer.
2.1.3	The lawful basis for collection and Processing of Personal Information must be recorded and maintained. The lawful basis for processing Personal Information by the Company (other than consent) may be contract, legal obligation, vital interest, public interest or legitimate interests.
2.1.4	Where Personal Information is being collected or Processed as part of a project, process or system, a data protection impact assessment ("DPIA") must be conducted. The DPIA is intended to identify, record and reduce the privacy risks associated with the project, process or system and must capture risk to the Data Subjects affected, and determine whether risk mitigation actions are required before the collection or Processing can take place.
2.1.5	Must use Personal Information only for the authorized purposes for which it was collected. If Personal Information is needed for an additional purpose, consent for the incremental purpose must be obtained or the lawful basis must be documented.
2.1.6	Must keep Personal Information current and accurate. It is the responsibility of each Data Subject to keep his or her Personal Information pertaining to home addresses, dependents, beneficiaries, or anything else that may affect that Data Subject's benefit status current. Where it is not possible for the Data Subject to maintain this Personal Information directly, he or she must notify the Company as soon as possible to request an update.

Requirement Number	Requirements
2.1.7	Must make use of protection methods such as locks, passwords, encryption, pseudonymisation and anonymisation to protect all Personal Information, in whatever form, within the Company's control. When no longer required, Personal Information will be made anonymous or destroyed in accordance with the Records Classification and Retention Schedule.
2.1.8	Closed circuit television recording devices are used across the Company's assets to protect the assets and people. Signs providing notice about the presence and use of such systems must be utilized. Images from closed circuit television recording devices must be managed as Restricted Information and in accordance with the requirements for classifying and protecting Business Information and Personal Information as defined in COUNTRIES-PRA-0197: Procedural Aid for Information Security Classification.
2.1.9	Must follow COUNTRIES-PRA-0285: Procedural Aid for Accessing Your Personal Information in order to either access one's own Personal Information held by the Company or to challenge its accuracy.
2.1.10	Must follow COUNTRIES-PRA-0286: Procedural Aid for Reporting a Privacy Complaint if a Data Subject wishes to challenge the Company's compliance with Applicable Privacy Legislation.
2.1.11	Must, as soon as reasonably possible and in any event within 24 hours of the discovery of the breach or suspected breach, report any breach or suspected breach of Applicable Privacy Legislation or this Standard, no matter how minor, by email or telephone, including information regarding the type of Personal Information involved, then known cause and extent of the breach, and the context of the affected Personal Information and the breach, to the Privacy Officer, or the applicable Company legal department, who will adhere to the Company's Personal Information Breach Response Plan in determining next steps in relation to the breach or suspected breach.
2.1.12	Must, where seeking a deviation from this Standard, consult with the Privacy Officer and thereafter seek authorization by the Chief Legal Officer or the VP – Human Resources.
Requirements for the Company	
2.1.13	Must ensure that appropriate training on the correct handling of Personal Information is provided, particularly to those in roles that will Process Special Categories of Personal Information, or that will Process significant volumes of Personal Information.
2.1.14	Must, where reasonably practicable and not inconsistent with Applicable Privacy Legislation, endeavor to comply with the highest standards set out in the Applicable Privacy Legislation, regardless of otherwise applicable jurisdiction.
2.1.15	Certain circumstances may require the transfer of Personal Information outside of a Data Subject's home country, such as, in connection with a Data Subject's employment, Processing the Personal Information together with the Company's related parties, including, but not limited to, CNOOC Limited and CNOOC International, as well as through use of a service provider, to collect, Process, use, disclose or store Personal Information. The Company must take reasonable measures to protect Personal Information while being collected, used, Processed or disclosed by related parties or other third parties.
2.1.16	Must have in place a Personal Information Breach Response Plan, which Breach Response Plan must be reviewed by the Privacy Officer at a minimal interval of every three years.

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 or delegate; every 3 years or when update required.	NMS.
Monitoring of data collection and Processing activities	Self-assessment and review of DPIAs.	Privacy Officer or delegate; as required, per project.	Livelink.
Tracking of Data Subject requests	Self-assessment; monitor for compliance with deadlines and completeness of response.	Privacy Officer or delegate; as required by the Company or by applicable Government Authority.	Livelink.
Testing associated processes, including, but not limited to, Personal Information Breach Response Plan	Test processes, including, but not limited to, compliance with deadlines and responsiveness.	Company corporate Audit department; periodic.	Livelink.

The Methods of Measurement, identified above, will be used as a foundation to determine whether this Standard is effective and efficient; and whether opportunities exist to further improve. Refer to the Continuous Improvement of CIMS Content – Review & Improve Business Process for further details.

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

3.0 REFERENCES AND RELATED INFORMATION

3.1 EXTERNAL REFERENCES

General Data Protection Regulation (EU) 2016/679

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

Personal Information Protection Act, SBC 2003, c 63

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

3.2 INTERNAL REFERENCES

GLOBAL-STD-0031	Standard for IT Acceptable Use
COUNTRIES-STD-0069	Standard for Information Management
GLOBAL-STD-0027	Standard for Confidential Information
COUNTRIES-PRA-0197	Procedural Aid for Information Security Classification
COUNTRIES-PRA-0285	Procedural Aid for Accessing Your Personal Information
COUNTRIES-PRA-0286	Procedural Aid for Reporting a Privacy Complaint

Records Classification and Retention Schedule

3.3 RELATED REFERENCES

Not Applicable

APPENDIX A: ROLES AND RESPONSIBILITIES

For a description of the CIMS Roles and Responsibilities, refer to the Standard for the CNOOC International Management System (CIMS)