BBNC Compliance Training
CUI / NIST SP 800-171

Bristol Bay Native Corporation

November 14, 2017

Executive Order 13556

- On November 4, 2010, **Executive Order 13556, entitled "*Controlled Unclassified Information,"*** was signed:

  "At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing."

Executive Order 13556
"CUI" is born…

"To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice."

CUI Defined

- Information that law, regulation, or government-wide policy requires safeguarding or disseminating controls (excluding information that is classified under Executive Order 13526, *Classified National Security Information*)
- Examples include information with privacy, security or proprietary interests, such as sensitive information regulated by statute, or operational information regulated by security frameworks, or information required by contract to be secure

Concise guidance: NIST SP 800-171

- Purpose of NIST SP 800-171 is to provide guidance – to define the security requirements - for protecting the confidentiality of CUI in nonfederal systems and organizations.
- Substance of NIST SP 800-171 is derived from the following:
  - Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems
  - FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
  - NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations; and
  - NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories

A simpler framework

- NIST SP 800-171 draws from the larger bucket of controls in the NIST SP 800-53 framework, but reduces the number of controls to something more manageable
- Goal is to provide those with authorized access to government data guidance to:
  - Identify *what* information within their systems is government controlled data; and
  - Determine *how* that data be segmented and protected

Security Requirement Families in NIST SP 800-171

- There are fourteen (14) families of security requirements for protecting the confidentiality of CUI in nonfederal information systems and organizations.

TABLE 1: SECURITY REQUIREMENT FAMILIES

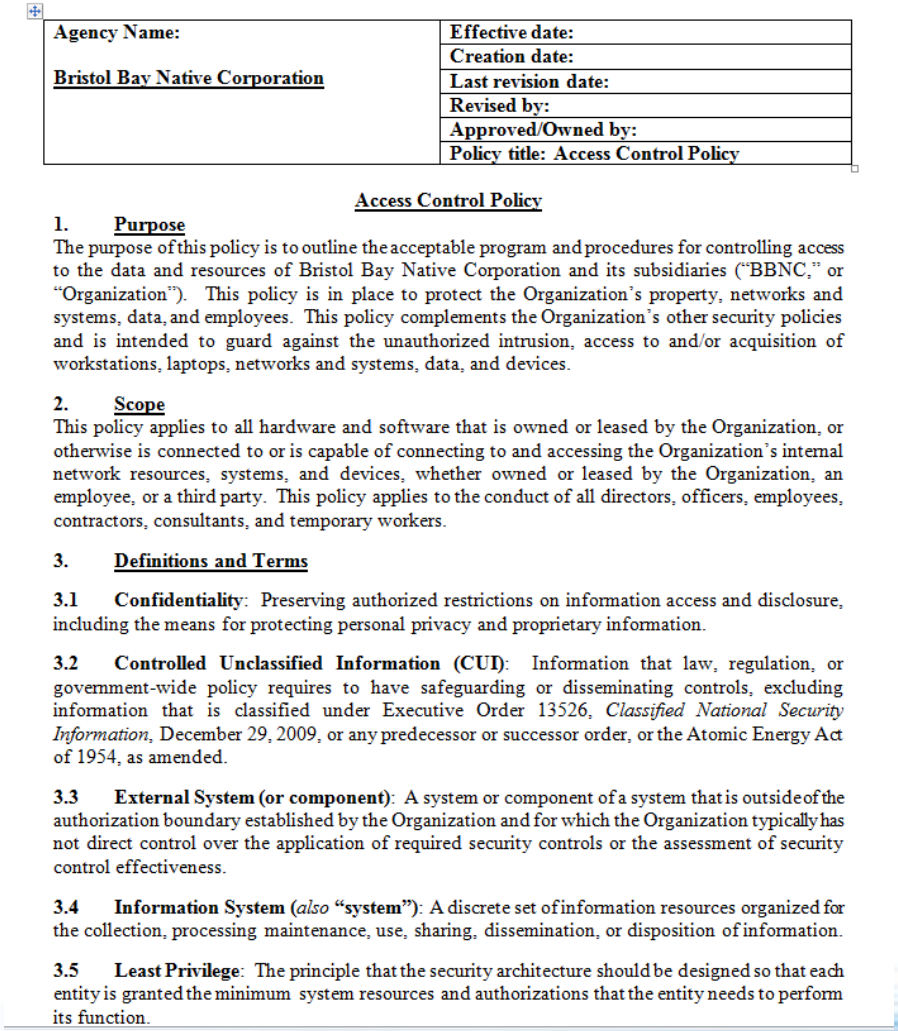
FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

Structure of the BBNC NIST SP 800-171 Policy Manual

- The manual is a compilation of 15 security policies
  - 14 policies mapped to the 14 families of security requirements in NIST SP 800-171
    - which contain a total of 109 security controls,
  - the BBNC Insider Threat Plan and Procedures
- The policies contain basic and derived requirements from *existing* and *recognized* security standards

Understanding the structure of each policy

- Policies are designed to be applicable to all subsidiaries
- Flexible enough for individualized implementation by each subsidiary
- First page of each policy contains header information about the effective date, version, and approval/owner of the policy



Agency Name:	Effective date:
	Creation date:
Bristol Bay Native Corporation	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Access Control Policy

Access Control Policy

1. Purpose

The purpose of this policy is to outline the acceptable program and procedures for controlling access to the data and resources of Bristol Bay Native Corporation and its subsidiaries ("BBNC," or "Organization"). This policy is in place to protect the Organization's property, networks and systems, data, and employees. This policy complements the Organization's other security policies and is intended to guard against the unauthorized intrusion, access to and/or acquisition of workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to all hardware and software that is owned or leased by the Organization, or otherwise is connected to or is capable of connecting to and accessing the Organization's internal network resources, systems, and devices, whether owned or leased by the Organization, an employee, or a third party. This policy applies to the conduct of all directors, officers, employees, contractors, consultants, and temporary workers.

3. Definitions and Terms

3.1 Confidentiality: Preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.

3.2 Controlled Unclassified Information (CUI): Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

3.3 External System (or component): A system or component of a system that is outside of the authorization boundary established by the Organization and for which the Organization typically has not direct control over the application of required security controls or the assessment of security control effectiveness.

3.4 Information System (*also* "system"): A discrete set of information resources organized for the collection, processing maintenance, use, sharing, dissemination, or disposition of information.

3.5 Least Privilege: The principle that the security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Understanding the structure of each policy

- Policies include sections on:
  - **Purpose**
  - **Scope**
  - **Definitions and Terms**
  - **Guiding Policy Principals**
  - **Basic Security Requirements**
  - **Policy Compliance**
  - **Implementation Procedures**
  - **Revision History**

4. Policy

4.1 Guiding Principles: In order to properly manage enterprise risk, the Organization must impose controls on who can access its data and other sensitive information. One of the most appropriate and basic means of controlling that access is to restrict it to only those authorized individuals who "need to know" or "need to access" in order to perform the responsibilities of their positions at the Organization. This restriction of access is an essential component of the Organization's information security program.

4.2 Basic Security Requirements

4.2.1 System access must be limited to authorized users, processes acting on behalf of authorized users, or devices (including other systems).

4.2.2 System access must be limited to the types of transactions and functions that authorized users are permitted to execute.

4.3 Controlling Access Based on the Need to Know/Approved Authorizations

4.3.1 The Organization must control the flow of CUI in accordance with approved authorizations.

4.3.2 The duties of individuals must be separated to reduce the risk of malevolent activity without collusion.

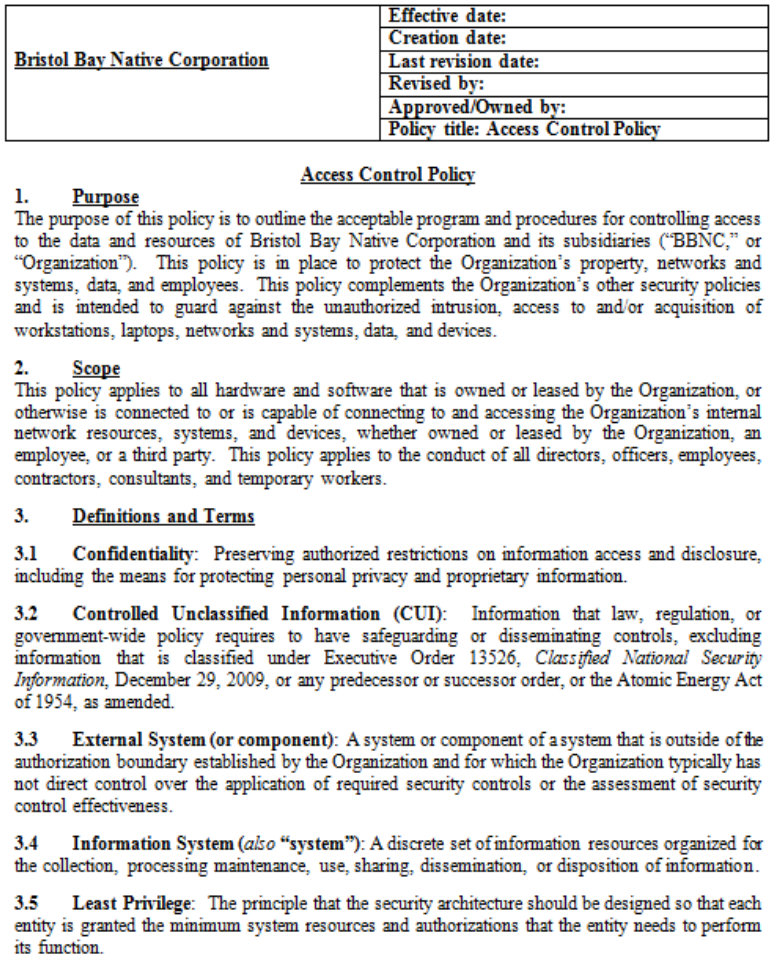
4.3.3 The Organization must employ the principle of least privilege, including for specific security functions and privileged accounts.

4.4 Use of Non-Privileged Accounts

4.4.1 The use of non-privileged accounts or roles is required when accessing non-security functions.

Policy #1: Access Control Policy

- Who is authorized to view the data?
- Principle of Least Privilege
- Access must be limited to
  - Authorized users
  - Types of transactions permitted for authorized users
- System must have sufficient controls to limit access
  - Monitor privileged accounts
  - Session locks
  - Encryption
  - Control remote access



Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Access Control Policy

Access Control Policy

1. Purpose

The purpose of this policy is to outline the acceptable program and procedures for controlling access to the data and resources of Bristol Bay Native Corporation and its subsidiaries ("BBNC," or "Organization"). This policy is in place to protect the Organization's property, networks and systems, data, and employees. This policy complements the Organization's other security policies and is intended to guard against the unauthorized intrusion, access to and/or acquisition of workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to all hardware and software that is owned or leased by the Organization, or otherwise is connected to or is capable of connecting to and accessing the Organization's internal network resources, systems, and devices, whether owned or leased by the Organization, an employee, or a third party. This policy applies to the conduct of all directors, officers, employees, contractors, consultants, and temporary workers.

3. Definitions and Terms

3.1 Confidentiality: Preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.

3.2 Controlled Unclassified Information (CUI): Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

3.3 External System (or component): A system or component of a system that is outside of the authorization boundary established by the Organization and for which the Organization typically has not direct control over the application of required security controls or the assessment of security control effectiveness.

3.4 Information System (*also* "system"): A discrete set of information resources organized for the collection, processing maintenance, use, sharing, dissemination, or disposition of information.

3.5 Least Privilege: The principle that the security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Policy #2: Awareness and Training Policy

- Are authorized users properly trained?
- Formalizes requirement for a training program on:
  - Security risks associated with user activities
  - Should include current threats including social engineering
  - Recognizing and reporting insider threat

Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Awareness & Training Policy

Awareness & Training Policy

1. Purpose

The purpose of this policy is to outline the acceptable programs and procedures for ensuring that Employees of Bristol Bay Native Corporation and its subsidiaries ("BBNC" or "Organization") are aware of, and receive training related to, the security risks associated with their activities and the implementation of policies relating to the security of the Organization's data and resources. The security awareness and training program helps the Organization document, communicate, and train Employees on security best practices and concepts. It also enables the Organization to manage certain risks resulting from lack of security awareness, communication, and training.

This policy is in place to protect the Organization's property, networks and systems, data, and Employees. This policy complements the Organization's other security policies and is intended to enable the Organization to guard against unauthorized intrusion, access to, and/or acquisition of Organization workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to the information security training that the Organization will require of all Employees including any and all users of Organization workstations, laptops, networks and systems, data, and devices. This training is intended increase Employee awareness about how to protect data that is processed, transmitted, or stored on Organization devices or on devices that are otherwise connected to, or are capable of connecting to, Organization networks and systems. All Organization Employees are responsible for adhering to this Awareness & Training Policy.

3. Definitions and Terms

3.1 Employees: The term "Employees" is defined to include any individual employed by the Organization, including but not limited to executives, directors, officers, managers, system administrators, contractors, consultants, and temporary workers.

4. Policy

4.1 Guiding Principles: In order to properly manage enterprise risk, the Organization must ensure that its Employees are aware of, and receive training related to, the security risks associated with their activities and the implementation of policies relating to the security of Organization data and resources. This is a critical component of the Organization's overall security posture as outside actors seeking to gain unauthorized access to its networks and systems may target its Employees through efforts such as spamming and phishing. An Employee's ability to recognize and detect outside actors attempting to gain unauthorized access to the Organization's system is a critical component of its information security program.

Policy #3: Audit and Accountability Policy

- Are logs enabled and records kept of authorized and unauthorized access?
- Requires
  - Audit logs to be maintained, monitored and analyzed
  - Actions of individual users to be uniquely traced to those users
  - Alerts if there is an audit process failure
  - Generation of reports to support on-demand analysis and reporting
  - Audit information and audit tools to be protected from unauthorized access, modification, and deletion

Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Audit & Accountability Policy

Audit & Accountability Policy

1. Purpose

The purpose of this policy is to outline the acceptable program and procedures for maintaining, monitoring, and analyzing of all audit logs generated by or on behalf of Bristol Bay Native Corporation and its subsidiaries ("BBNC," or "Organization"), in order to manage risks from inadequate event logging and monitoring. The rules contained in this policy are in place to protect the Organization's property, networks and systems, data and employees. These rules complement the Organization's other security policies, and are intended to guard against the unauthorized intrusion, access to and/or acquisition of workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to all audit logs that are or should be generated by or on behalf of the Organization, arising from the transmission of data through hardware and software that is owned or leased by the Organization, or otherwise is connected to or is capable of connecting to and accessing the Organization's internal network resources, systems, and devices, whether owned or leased by the Organization, an employee, or a third party. This policy applies to the conduct of all directors, officers, employees, contractors, consultants, and temporary workers.

3. Definitions and Terms

3.1 Audit Log: A chronological record of system activities, including records of system accesses and operations performed in a given period.

3.2 Audit Record: An individual entry in an audit log related to an audited event.

3.3 Information System (*also* "system"): A discrete set of information resources organized for the collection, processing maintenance, use, sharing, dissemination, or disposition of information.

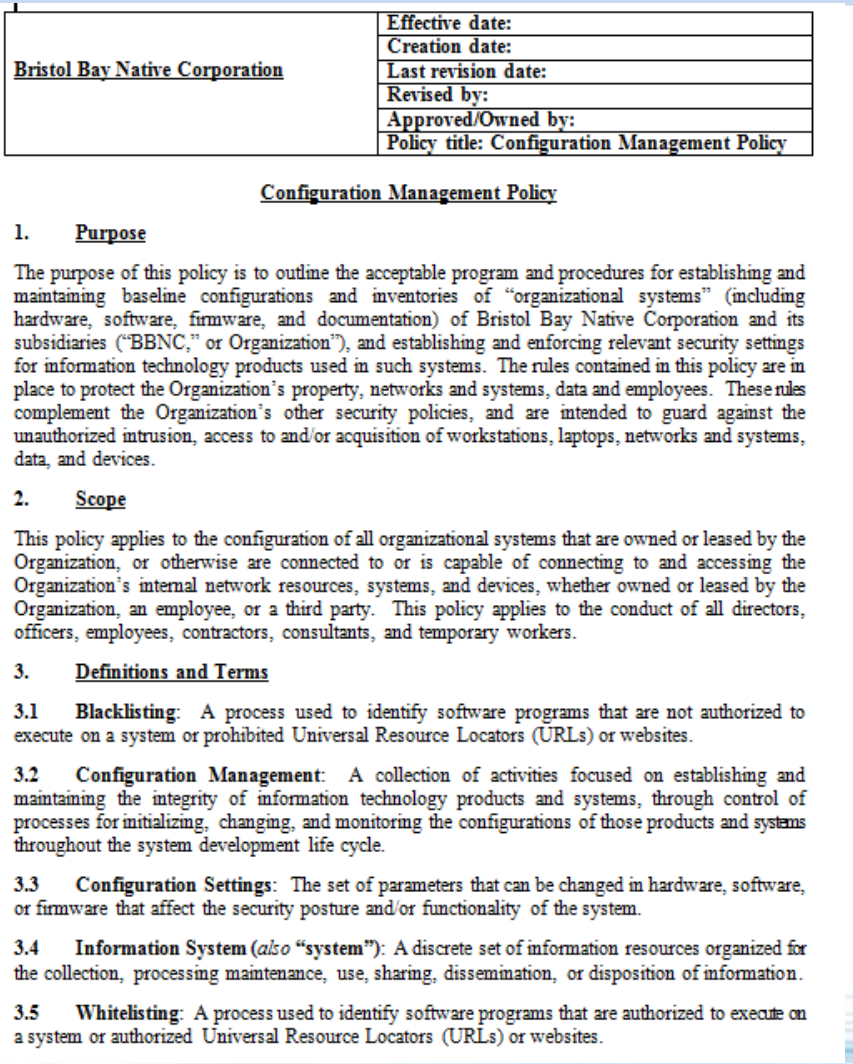
3.4 User: Individual, or (system) process active on behalf of an individual, authorized to access a system.

4. Policy

4.1 Guiding Principles: In order to safeguard the security and the integrity of its facilities, devices, data, and systems, it is extremely important that all audit logs be enabled to capture all access to and use of the Organization's facilities, workstations, laptops, networks and systems, devices, and data. The continuous maintenance, monitoring and analysis of the Organization's audit logs is a critical component of the information security program.

Policy #4: Configuration Management Policy

- Intended to limit attack surface by preventing the use of nonessential programs, functions, ports, protocols, and services
- Focuses on the principal of least functionality by configuring information systems to provide only *essential* capabilities
- Supports creation of a "standard" image, where feasible; removal of bloatware



Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Configuration Management Policy

Configuration Management Policy

1. Purpose

The purpose of this policy is to outline the acceptable program and procedures for establishing and maintaining baseline configurations and inventories of "organizational systems" (including hardware, software, firmware, and documentation) of Bristol Bay Native Corporation and its subsidiaries ("BBNC," or Organization"), and establishing and enforcing relevant security settings for information technology products used in such systems. The rules contained in this policy are in place to protect the Organization's property, networks and systems, data and employees. These rules complement the Organization's other security policies, and are intended to guard against the unauthorized intrusion, access to and/or acquisition of workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to the configuration of all organizational systems that are owned or leased by the Organization, or otherwise are connected to or is capable of connecting to and accessing the Organization's internal network resources, systems, and devices, whether owned or leased by the Organization, an employee, or a third party. This policy applies to the conduct of all directors, officers, employees, contractors, consultants, and temporary workers.

3. Definitions and Terms

3.1 Blacklisting: A process used to identify software programs that are not authorized to execute on a system or prohibited Universal Resource Locators (URLs) or websites.

3.2 Configuration Management: A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

3.3 Configuration Settings: The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system.

3.4 Information System (*also* "system"): A discrete set of information resources organized for the collection, processing maintenance, use, sharing, dissemination, or disposition of information.

3.5 Whitelisting: A process used to identify software programs that are authorized to execute on a system or authorized Universal Resource Locators (URLs) or websites.

Policy #5: Identification and Authentication Policy

- Requires identification of all users, processes acting on behalf of users, and devices
- Requires identities to be authenticated
- Requires multi-factor authentication for network access to privileged and non-privileged accounts
- Requires minimum password complexity and change of character requirements when new passwords are created
- Passwords must be encrypted when stored or transmitted
- Recent attacks attributable to storage of passwords in clear text

Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Identification and Authentication Policy

Identification and Authentication Policy

1. Purpose

The purpose of this policy is to outline the acceptable program and procedures for monitoring and controlling the accounts of persons authorized to access data or any portion of the information systems of Bristol Bay Native Corporation and its subsidiaries ("BBNC" or "Organization"). The rules contained in this policy are in place to protect the Organization's property, networks and systems, data and employees. These rules complement the Organization's other security policies, and are intended to guard against the unauthorized intrusion, access to and/or acquisition of workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to all user accounts on the Organization's information system, whether they are currently active, deactivated, or disabled, if they may potentially be capable of connecting to and accessing the Organization's internal network resources, systems, and devices, whether owned or leased by the Organization, an employee, or a third party. This policy applies to the conduct of all directors, officers, employees, contractors, consultants, and temporary workers.

3. Definitions and Terms

3.1 Identifier: Unique data used to represent a person's identity and associated attributes. Examples of identifiers include: a name; a credit card number; a unique label used by a system to indicate a specific entity, object, or group; etc.

3.2 Local Access: Access to a system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

3.3 Multi-Factor Authentication: Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g. PIN, password); something you have (eg. cryptographic identification device, token); or something you are (e.g. biometrics).

3.4 Network Access: Access to a system by a user (or process acting on behalf of a user) communicating through a network (e.g. local area network ("LAN"), wide area network ("WAN"), the Internet, etc.).

3.5 Privileged Account: A system account with authorizations of a privileged user.

3.6 Privileged User: A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Policy #6: Incident Response Policy

- Recognizes that preparing for an information security incident and the business interruptions that may follow is a critical part of information security
- Requires written incident response plan aligned with specific needs and operations that includes adequate preparation, detection, analysis, containment, recovery, and user response activities
- Requires an escalation procedure for internal and external reporting
- Requires plan to be tested at least annually through tabletop exercise

Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Incident Response Policy

Incident Response Policy

1. Purpose

The purpose of this policy is to outline the acceptable program and procedures for the planning and management related to incident response and business continuity. The rules contained in this policy are in place to protect the property, networks and systems, data and employees of Bristol Bay Native Corporation and its subsidiaries ("BBNC" or "Organization"). These rules complement the Organization's other security policies, and are intended to guard against the unauthorized intrusion, access to and/or acquisition of workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to the development and implementation of incident response and business continuity plans. This policy applies to the conduct of all directors, officers, employees, contractors, consultants, and temporary workers.

3. Definitions and Terms

3.1 Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

3.2 Information System (*also* **"system"**): A discrete set of information resources organized for the collection, processing maintenance, use, sharing, dissemination, or disposition of information.

4. Policy

4.1 Guiding Principles: Conventional wisdom is that it is not a matter of "if" but "when" an Organization will be affected by an information security incident that may compromise sensitive data and/or affect normal business operations. The most important action an Organization can take in light of the inevitable information security incident is to prepare for it. The preparation for an information security incident, and the business interruptions that may follow, is a critical component of the Organization's information security program.

4.2 Basic Security Requirements

4.2.1 The Organization must establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

Policy #7: Maintenance Policy

- The health of information systems depends upon regular maintenance
- Requires the maintenance of all systems, devices, and supporting systems, and requires effective controls throughout the process
- Requires media to be sanitized if removed from premises for maintenance
- Requires protective measures be put in place for tools and individuals used to conduct maintenance
- Requires multi-factor authentication for non-local maintenance

Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Maintenance Policy

Maintenance Policy

1. Purpose

The purpose of this policy is to outline the acceptable program and procedures for maintaining and repairing the organizational system assets of Bristol Bay Native Corporation and its subsidiaries ("BBNC" or "Organization"). The rules contained in this policy are in place to protect the Organization's property, networks and systems, data and employees. These rules complement the Organization's other security policies, and are intended to guard against the unauthorized intrusion, access to and/or acquisition of workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to the continued maintenance and repair of the organizational system assets within and utilized by the Organization. This policy applies to the conduct of all directors, officers, employees, contractors, consultants, and temporary workers.

3. Definitions and Terms

3.1 Controlled Unclassified Information (CUI): Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

3.2 External Network: A network not controlled by the organization.

3.3 Information System (*also* "system"): A discrete set of information resources organized for the collection, processing maintenance, use, sharing, dissemination, or disposition of information.

3.4 Internal Network: A network where establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or the cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.

3.5 Malicious Code: Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code, or "malware."

Policy #8: Media Protection Policy

- Recognizes critical need to protect CUI stored on media devices
- Requires access to CUI to be limited to authorized users
- Requires system media containing CUI to be sanitized before being disposed or released for reuse
- Requires media containing CUI to be encrypted during transport outside of controlled areas
- Prohibits used of portable storage devices with no identifiable owner
- Requires protection of backup CUI that is stored, housed, or maintained off premises

Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Media Protection Policy

Media Protection Policy

1. Purpose

The purpose of this policy is to outline the acceptable program and procedures for the protection of media containing sensitive data created, processed, or stored by or on behalf of Bristol Bay Native Corporation and its subsidiaries ("BBNC" or "the Organization") from unauthorized or impermissible access, acquisition, alteration, modification, disclosure or destruction. The rules contained in this policy are in place to protect the Organization's property, networks and systems, data and employees. These rules complement the Organization's other security policies, and are intended to guard against the unauthorized intrusion, access to and/or acquisition of workstations, laptops, networks and systems, media, data, and devices.

2. Scope

This policy applies to the media created, processed, transmitted or stored by or on behalf of the Organization. This policy applies to the conduct of all directors, officers, employees, contractors, consultants, and temporary workers.

3. Definitions and Terms

3.1 Confidentiality: Preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.

3.2 Controlled Unclassified Information (CUI): Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

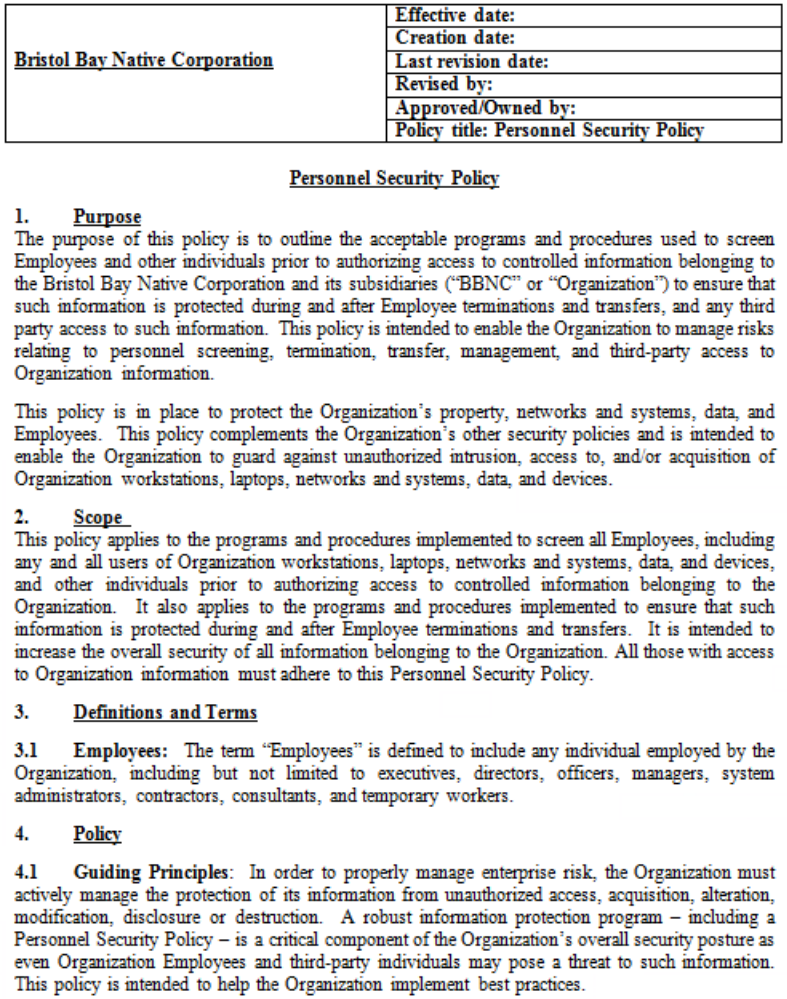
3.3 Information System (*also* **"system"**): A discrete set of information resources organized for the collection, processing maintenance, use, sharing, dissemination, or disposition of information.

3.4 Media: Physical devices or writing services including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration ("LSI") memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system.

3.5 System Component: A discrete, identifiable information technology asset (hardware, software, firmware) that represents a building block of a system. System components include commercial information technology products.

Policy #9: Personnel Security Policy

- How are employees screened before gaining access to CUI?
- Requires screening of all potential authorized users
- Requires CUI to be adequately protected *during* and *after* personnel actions such as terminations and transfers
- Terminated employees whose credentials have not been disabled are the source of numerous incidents …



Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Personnel Security Policy

Personnel Security Policy

1. Purpose

The purpose of this policy is to outline the acceptable programs and procedures used to screen Employees and other individuals prior to authorizing access to controlled information belonging to the Bristol Bay Native Corporation and its subsidiaries ("BBNC" or "Organization") to ensure that such information is protected during and after Employee terminations and transfers, and any third party access to such information. This policy is intended to enable the Organization to manage risks relating to personnel screening, termination, transfer, management, and third-party access to Organization information.

This policy is in place to protect the Organization's property, networks and systems, data, and Employees. This policy complements the Organization's other security policies and is intended to enable the Organization to guard against unauthorized intrusion, access to, and/or acquisition of Organization workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to the programs and procedures implemented to screen all Employees, including any and all users of Organization workstations, laptops, networks and systems, data, and devices, and other individuals prior to authorizing access to controlled information belonging to the Organization. It also applies to the programs and procedures implemented to ensure that such information is protected during and after Employee terminations and transfers. It is intended to increase the overall security of all information belonging to the Organization. All those with access to Organization information must adhere to this Personnel Security Policy.

3. Definitions and Terms

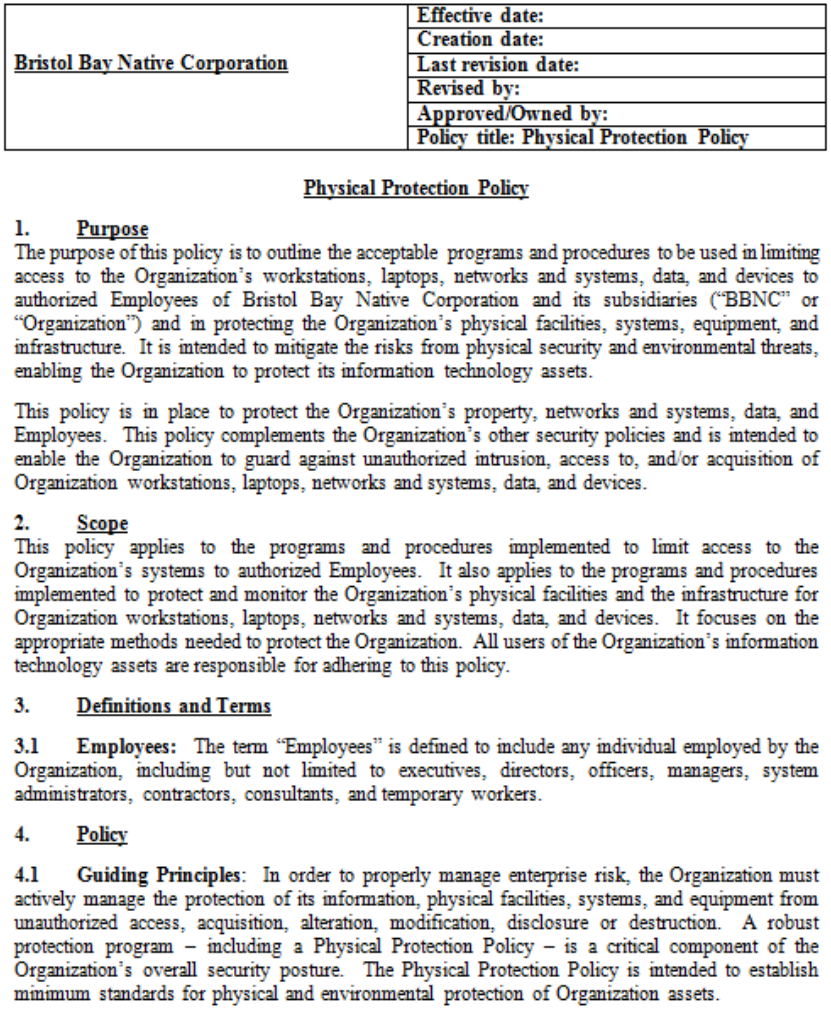
3.1 Employees: The term "Employees" is defined to include any individual employed by the Organization, including but not limited to executives, directors, officers, managers, system administrators, contractors, consultants, and temporary workers.

4. Policy

4.1 Guiding Principles: In order to properly manage enterprise risk, the Organization must actively manage the protection of its information from unauthorized access, acquisition, alteration, modification, disclosure or destruction. A robust information protection program – including a Personnel Security Policy – is a critical component of the Organization's overall security posture as even Organization Employees and third-party individuals may pose a threat to such information. This policy is intended to help the Organization implement best practices.

Policy #10: Physical Protection Policy

- How physical access to premises and CUI controlled?
- Physical security is a critical aspect of protecting CUI
- Requires
  - Visitors to be escorted
  - Audit logs of physical access to premises and information assets
  - Control of physical access devices



Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Physical Protection Policy

Physical Protection Policy

1. Purpose

The purpose of this policy is to outline the acceptable programs and procedures to be used in limiting access to the Organization's workstations, laptops, networks and systems, data, and devices to authorized Employees of Bristol Bay Native Corporation and its subsidiaries ("BBNC" or "Organization") and in protecting the Organization's physical facilities, systems, equipment, and infrastructure. It is intended to mitigate the risks from physical security and environmental threats, enabling the Organization to protect its information technology assets.

This policy is in place to protect the Organization's property, networks and systems, data, and Employees. This policy complements the Organization's other security policies and is intended to enable the Organization to guard against unauthorized intrusion, access to, and/or acquisition of Organization workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to the programs and procedures implemented to limit access to the Organization's systems to authorized Employees. It also applies to the programs and procedures implemented to protect and monitor the Organization's physical facilities and the infrastructure for Organization workstations, laptops, networks and systems, data, and devices. It focuses on the appropriate methods needed to protect the Organization. All users of the Organization's information technology assets are responsible for adhering to this policy.

3. Definitions and Terms

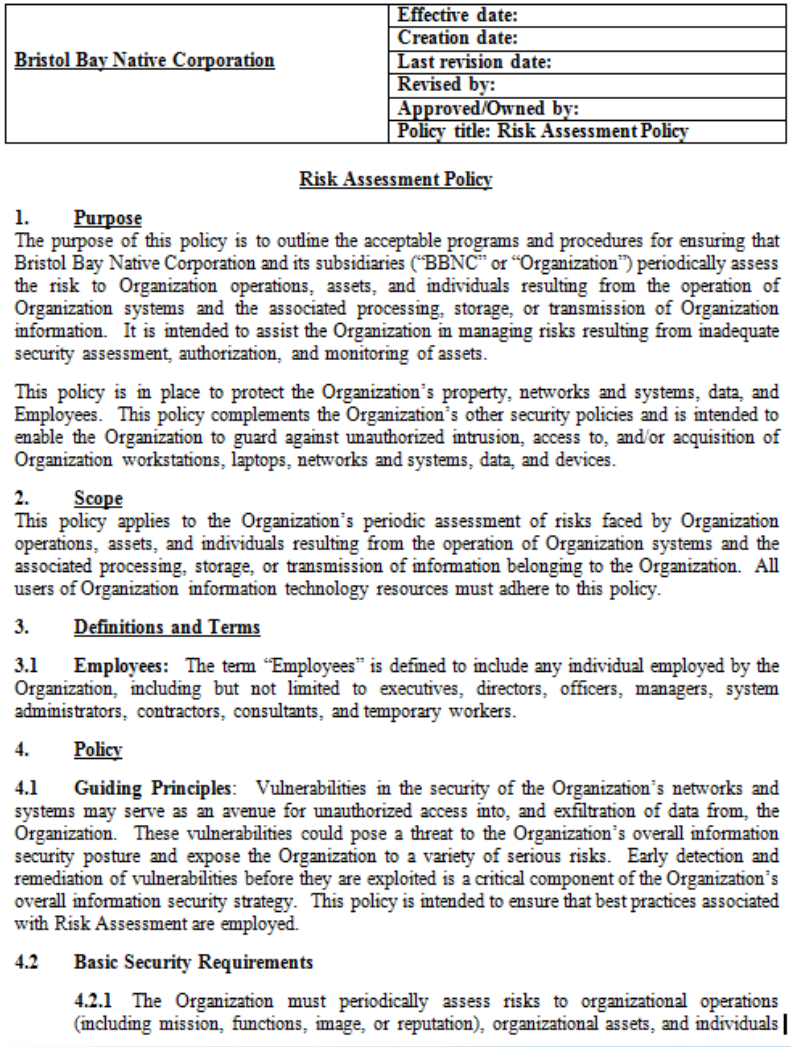
3.1 Employees: The term "Employees" is defined to include any individual employed by the Organization, including but not limited to executives, directors, officers, managers, system administrators, contractors, consultants, and temporary workers.

4. Policy

4.1 Guiding Principles: In order to properly manage enterprise risk, the Organization must actively manage the protection of its information, physical facilities, systems, and equipment from unauthorized access, acquisition, alteration, modification, disclosure or destruction. A robust protection program – including a Physical Protection Policy – is a critical component of the Organization's overall security posture. The Physical Protection Policy is intended to establish minimum standards for physical and environmental protection of Organization assets.

Policy #11: Risk Assessment Policy

- Highlights the importance of conducting:
  - Vulnerability scans
  - Vulnerability remediation
- Requires periodic scans no less than quarterly
- Requires system risk assessment annually
- Requires remediation of vulnerabilities
- Many recent breaches have been attributable to the failure to conduct timely scanning and remediation!



Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Risk Assessment Policy

Risk Assessment Policy

1. Purpose

The purpose of this policy is to outline the acceptable programs and procedures for ensuring that Bristol Bay Native Corporation and its subsidiaries ("BBNC" or "Organization") periodically assess the risk to Organization operations, assets, and individuals resulting from the operation of Organization systems and the associated processing, storage, or transmission of Organization information. It is intended to assist the Organization in managing risks resulting from inadequate security assessment, authorization, and monitoring of assets.

This policy is in place to protect the Organization's property, networks and systems, data, and Employees. This policy complements the Organization's other security policies and is intended to enable the Organization to guard against unauthorized intrusion, access to, and/or acquisition of Organization workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to the Organization's periodic assessment of risks faced by Organization operations, assets, and individuals resulting from the operation of Organization systems and the associated processing, storage, or transmission of information belonging to the Organization. All users of Organization information technology resources must adhere to this policy.

3. Definitions and Terms

3.1 Employees: The term "Employees" is defined to include any individual employed by the Organization, including but not limited to executives, directors, officers, managers, system administrators, contractors, consultants, and temporary workers.

4. Policy

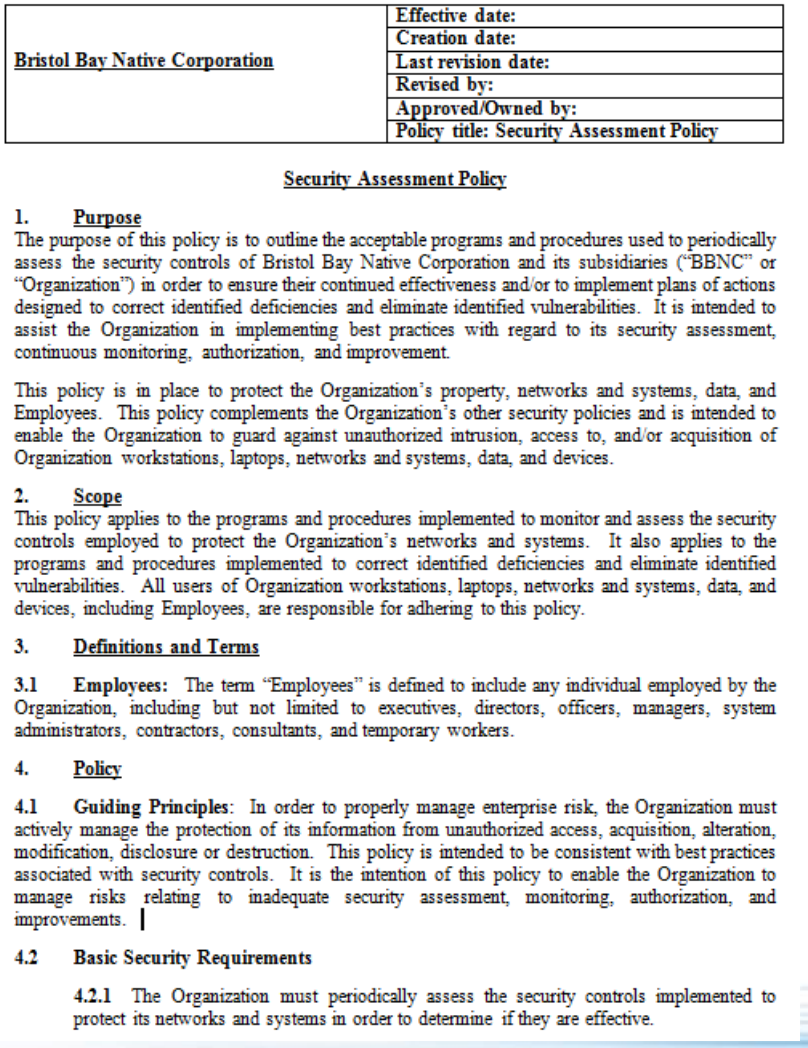
4.1 Guiding Principles: Vulnerabilities in the security of the Organization's networks and systems may serve as an avenue for unauthorized access into, and exfiltration of data from, the Organization. These vulnerabilities could pose a threat to the Organization's overall information security posture and expose the Organization to a variety of serious risks. Early detection and remediation of vulnerabilities before they are exploited is a critical component of the Organization's overall information security strategy. This policy is intended to ensure that best practices associated with Risk Assessment are employed.

4.2 Basic Security Requirements

4.2.1 The Organization must periodically assess risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals

Policy #12: Security Assessment Policy

- Highlights the importance of periodically assessing and improving security controls
- Requires the organization to conduct initial and periodic risk assessments using FIPS 199
- Requires a plan of action to correct deficiencies and/or eliminate system vulnerabilities
- Requires review of system boundaries, system environments of operations, and implementation of security controls and their connections with other systems



Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Security Assessment Policy

Security Assessment Policy

1. Purpose

The purpose of this policy is to outline the acceptable programs and procedures used to periodically assess the security controls of Bristol Bay Native Corporation and its subsidiaries ("BBNC" or "Organization") in order to ensure their continued effectiveness and/or to implement plans of actions designed to correct identified deficiencies and eliminate identified vulnerabilities. It is intended to assist the Organization in implementing best practices with regard to its security assessment, continuous monitoring, authorization, and improvement.

This policy is in place to protect the Organization's property, networks and systems, data, and Employees. This policy complements the Organization's other security policies and is intended to enable the Organization to guard against unauthorized intrusion, access to, and/or acquisition of Organization workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to the programs and procedures implemented to monitor and assess the security controls employed to protect the Organization's networks and systems. It also applies to the programs and procedures implemented to correct identified deficiencies and eliminate identified vulnerabilities. All users of Organization workstations, laptops, networks and systems, data, and devices, including Employees, are responsible for adhering to this policy.

3. Definitions and Terms

3.1 Employees: The term "Employees" is defined to include any individual employed by the Organization, including but not limited to executives, directors, officers, managers, system administrators, contractors, consultants, and temporary workers.

4. Policy

4.1 Guiding Principles: In order to properly manage enterprise risk, the Organization must actively manage the protection of its information from unauthorized access, acquisition, alteration, modification, disclosure or destruction. This policy is intended to be consistent with best practices associated with security controls. It is the intention of this policy to enable the Organization to manage risks relating to inadequate security assessment, monitoring, authorization, and improvements.

4.2 Basic Security Requirements

4.2.1 The Organization must periodically assess the security controls implemented to protect its networks and systems in order to determine if they are effective.

Policy #13: System and Communication Protection Policy

- Highlights the importance of monitoring and protecting organization communications
- Requires monitoring and protection of communications at external boundaries and key internal boundaries
- Requires standards for architectural design, software development, and system engineering principles in order to promote information security
- Requires network segmentation, access control and encryption to protect communications

Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: Systems And Communications Protection Policy

Systems and Communications Protection Policy

1. Purpose

The purpose of this policy is to outline the acceptable programs and procedures used to monitor, control, and protect communications of Bristol Bay Native Corporation and its subsidiaries ("BBNC" or "Organization") and to employ a number of measures to promote effective information security. This policy applies to both internal and external Organization communications and is intended to enable the Organization to manage risks resulting from vulnerable system configurations, denial of service, and/or data communication and transfer.

This policy is in place to protect the Organization's property, networks and systems, data, and Employees. This policy complements the Organization's other security policies and is intended to enable the Organization to guard against unauthorized intrusion, access to, and/or acquisition of Organization workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to the programs and procedures implemented to monitor, control, and protect both internal and external Organization communications. All users of Organization workstations, laptops, networks and systems, data, and devices, including Employees, are responsible for adhering to this policy.

3. Definitions and Terms

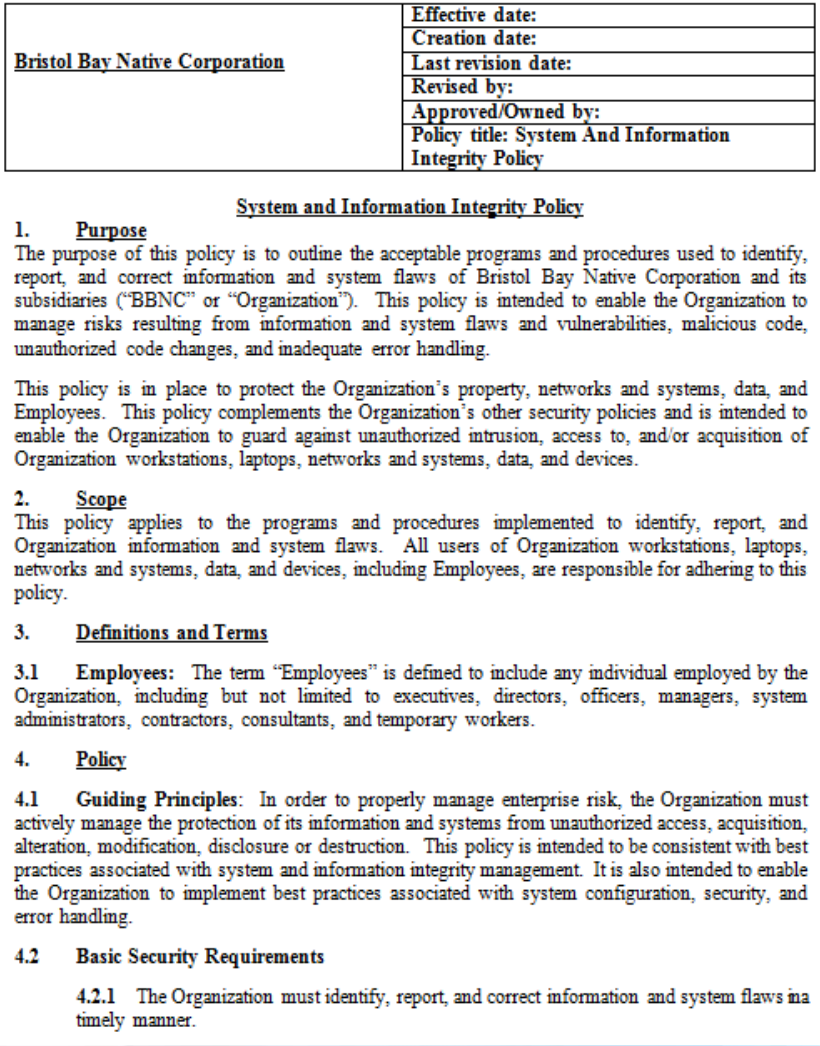
3.1 Employees: The term "Employees" is defined to include any individual employed by the Organization, including but not limited to executives, directors, officers, managers, system administrators, contractors, consultants, and temporary workers.

4. Policy

4.1 Guiding Principles: In order to properly manage enterprise risk, the Organization must actively manage the protection of its information from unauthorized access, acquisition, alteration, modification, disclosure or destruction. This policy is intended to be consistent with best practices associated with information security management. It is also intended to enable the Organization to implement best practices associated with system configuration as well as data communication and transfer .

Policy #14: System and Information Integrity Policy

- Includes the requirement to:
  - Identify, report, and correct flaws in a timely manner
  - Protect Organization from malicious code at appropriate locations
  - Monitor alerts and advisories and take appropriate action in response
- Formalizes the requirement to monitor and take action against threats
- Highlights critical need for skills training and education!



Bristol Bay Native Corporation	Effective date:
	Creation date:
	Last revision date:
	Revised by:
	Approved/Owned by:
	Policy title: System And Information Integrity Policy

System and Information Integrity Policy

1. Purpose

The purpose of this policy is to outline the acceptable programs and procedures used to identify, report, and correct information and system flaws of Bristol Bay Native Corporation and its subsidiaries ("BBNC" or "Organization"). This policy is intended to enable the Organization to manage risks resulting from information and system flaws and vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling.

This policy is in place to protect the Organization's property, networks and systems, data, and Employees. This policy complements the Organization's other security policies and is intended to enable the Organization to guard against unauthorized intrusion, access to, and/or acquisition of Organization workstations, laptops, networks and systems, data, and devices.

2. Scope

This policy applies to the programs and procedures implemented to identify, report, and Organization information and system flaws. All users of Organization workstations, laptops, networks and systems, data, and devices, including Employees, are responsible for adhering to this policy.

3. Definitions and Terms

3.1 Employees: The term "Employees" is defined to include any individual employed by the Organization, including but not limited to executives, directors, officers, managers, system administrators, contractors, consultants, and temporary workers.

4. Policy

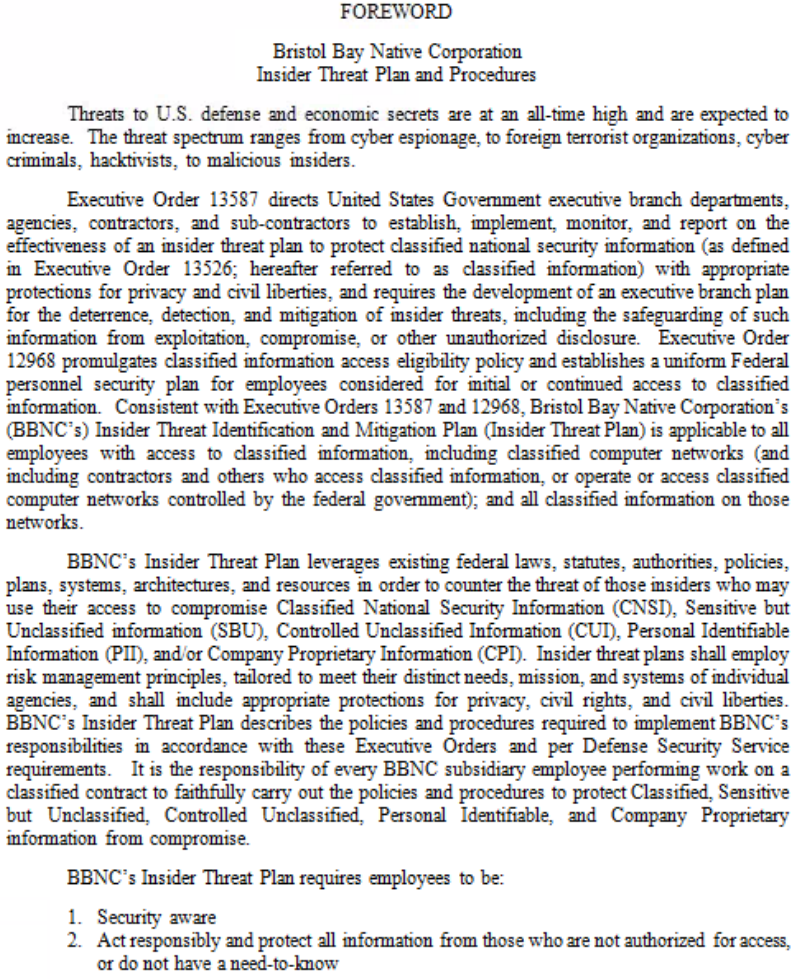
4.1 Guiding Principles: In order to properly manage enterprise risk, the Organization must actively manage the protection of its information and systems from unauthorized access, acquisition, alteration, modification, disclosure or destruction. This policy is intended to be consistent with best practices associated with system and information integrity management. It is also intended to enable the Organization to implement best practices associated with system configuration, security, and error handling.

4.2 Basic Security Requirements

4.2.1 The Organization must identify, report, and correct information and system flaws in a timely manner.

Policy #15: Insider Threat Protection Policy

- BBNC's Insider Threat Plan requires employees to be:
  - Security aware
  - Act responsibly and protect all information from those who are not authorized for access, or do not have a need-to-know
  - Report suspicious activity and/or adverse information as outlined in BBNC's Insider Threat Plan
- If you have questions or suggestions concerning the Insider Threat Plan or other security related issues, direct them to your respective Facility Security Officer (FSO)



FOREWORD

Bristol Bay Native Corporation
Insider Threat Plan and Procedures

Threats to U.S. defense and economic secrets are at an all-time high and are expected to increase. The threat spectrum ranges from cyber espionage, to foreign terrorist organizations, cyber criminals, hacktivists, to malicious insiders.

Executive Order 13587 directs United States Government executive branch departments, agencies, contractors, and sub-contractors to establish, implement, monitor, and report on the effectiveness of an insider threat plan to protect classified national security information (as defined in Executive Order 13526; hereafter referred to as classified information) with appropriate protections for privacy and civil liberties, and requires the development of an executive branch plan for the deterrence, detection, and mitigation of insider threats, including the safeguarding of such information from exploitation, compromise, or other unauthorized disclosure. Executive Order 12968 promulgates classified information access eligibility policy and establishes a uniform Federal personnel security plan for employees considered for initial or continued access to classified information. Consistent with Executive Orders 13587 and 12968, Bristol Bay Native Corporation's (BBNC's) Insider Threat Identification and Mitigation Plan (Insider Threat Plan) is applicable to all employees with access to classified information, including classified computer networks (and including contractors and others who access classified information, or operate or access classified computer networks controlled by the federal government); and all classified information on those networks.

BBNC's Insider Threat Plan leverages existing federal laws, statutes, authorities, policies, plans, systems, architectures, and resources in order to counter the threat of those insiders who may use their access to compromise Classified National Security Information (CNSI), Sensitive but Unclassified information (SBU), Controlled Unclassified Information (CUI), Personal Identifiable Information (PII), and/or Company Proprietary Information (CPI). Insider threat plans shall employ risk management principles, tailored to meet their distinct needs, mission, and systems of individual agencies, and shall include appropriate protections for privacy, civil rights, and civil liberties. BBNC's Insider Threat Plan describes the policies and procedures required to implement BBNC's responsibilities in accordance with these Executive Orders and per Defense Security Service requirements. It is the responsibility of every BBNC subsidiary employee performing work on a classified contract to faithfully carry out the policies and procedures to protect Classified, Sensitive but Unclassified, Controlled Unclassified, Personal Identifiable, and Company Proprietary information from compromise.

BBNC's Insider Threat Plan requires employees to be:

1. Security aware
2. Act responsibly and protect all information from those who are not authorized for access, or do not have a need-to-know

Who will insure compliance?

- Contracting officers must insure compliance, *but* it will require BBNC to educate and train contracting officers about how BBNC is being compliant.
- A third party will assess systems to verify compliance - self-certification will not be enough

What will contracting officers require under 800-171?

- 3rd party security assessments. Contracting officers will ask for due diligence:
  - What have you done?
  - How did you do it?
  - Who did it for you?
  - How can you prove it to me?
- Be prepared to say, “Yes, I’m 171 compliant. Here’s my:
  - Identifiable data
  - Policies and procedures
  - Incident response plan
  - Everything needed to verify my compliance

Compliance and enforcement of 800-171 Managing third party vendors

- Every contract must address CUI
- Contracting officers will ask, “What’s your SP 800-171 plan?”
- If systems generally meet the requirements of SP 800-171, but certain systems may be or appear to be controlled differently, prepare to justify why those efforts are the functional equivalent

Other considerations and preparation

- Identify what the CUI data is, and determine which systems contain it
- Perform a gap analysis on systems, and be prepared to explain how CUI will be protected
- Be prepared to explain organizational plan for compliance, including any gaps in the plan

Compliance principles for discussion

- Contractors may do business with a number of entities in the supply chain
  - “Downstream” (systems integrators and resellers) and also “upstream” (manufacturers, OEMs, software publishers)
- All are responsible for compliance and must comply with standards!
- Long term strategy should be to extend systems upstream and downstream wherever possible, so partners and suppliers don’t have to worry about their systems
- Overall Goal: to have government data securely stored in a compliant environment, and *accessed* by those who need access while minimizing the risk of breaches

Sean B. Hoar
Chair, Data Privacy and Cybersecurity Practice
sean.hoar@lewisbrisbois.com
971-712-2795 (Office)
503-459-7707 (Mobile)

LEWIS BRISBOIS
BISGAARD & SMITH LLP

Disclaimer
Any information provided by the speakers and/or Lewis Brisbois Bisgaard & Smith, LLP [collectively "Lewis Brisbois"] in or from this presentation is for informational purposes and shall not be considered as legal advice from Lewis Brisbois or as creating a professional client relationship between the person and Lewis Brisbois or any of its attorneys or staff. This presentation contains general information and may not reflect current law or legal developments. Any person viewing or receiving information from this presentation should not act or refrain from acting on the basis of any such information, but instead should seek appropriate legal advice from a qualified professional. Lewis Brisbois expressly disclaims any intent to provide legal advice to, or form a client relationship with any person based on the viewing of this presentation. Furthermore, Lewis Brisbois disclaims any liability whatsoever with respect to any actions taken or not taken by any person based on the content of this presentation or any information contained herein.