Cybersecurity and Acceptable Use Policy

Policy Statement

South Bow is committed to safeguarding its Digital Assets, Information, and systems by ensuring the secure, lawful, and responsible use of technology. This policy establishes the standards and behaviors expected of all Team Members and Excluded Contractors to protect Company Data, uphold cybersecurity rules, and maintain compliance with laws, regulations, and internal governance.

Scope

The policy applies to all South Bow Team Members and Contractors in all jurisdictions where South Bow operates.

It governs the access, use, and management of Company Digital Assets, Accounts, systems, and Information, whether accessed on-site, remotely, or via approved devices and networks.

Principles

1 Integrity of Information and systems

1.1 Protect South Bow's Digital Assets and Information from unauthorized access, disclosure, alteration, loss, or destruction.

1.2 All use of Digital Assets, Digital Information, and Accounts must comply with applicable laws, regulations, and South Bow's governance frameworks, including the Code of Business Ethics (COBE) Policy, Information Management Policy, Protection of Personal Information Policy, Inter-Affiliate Rules, and other Company policies.

2 Confidentiality and privacy

2.1 Safeguard confidential, personal, and sensitive Information at all times, ensuring it is not stored, transmitted, or disclosed through unapproved channels or devices, including online personal accounts.

3 Accountability and access control

3.1 Use only Company-approved systems and networks, with access granted based on the Principle of Least Privilege and subject to monitoring and review.

4 Cybersecurity vigilance

4.1 Follow Company cybersecurity standards, exercise diligence against threats such as phishing or Social Engineering, and report suspected incidents immediately.

5 Artificial Intelligence (AI) and emerging technologies

5.1 Use only Company-approved tools and platforms, in alignment with IT Operations and Cybersecurity guidance, and South Bow's AI Policy.

Implementation

1 Use of South Bow Digital Assets

1.1 All users must comply with Company cybersecurity standards, including password requirements, encryption standards, and system configuration rules.

1.2 Security settings must not be modified without written authorization from the Cybersecurity Office (CSO).

1.3 Company Information must not be processed in external applications including AI tools or disclosed to third parties without prior approval from IT Operations and the CSO.

1.4 Cybersecurity threats are to be addressed in full alignment with guidance from the CSO or designated authority. Only official communications from the CSO sent via South Bow's Cyber Safety account (cyber.safety@southbow.com) or CSO's mailbox (cybersecurity.office@southbow.com) are to be recognized as legitimate.

1.5 Only Company-approved hardware, software, and networks may be used to access or handle Company Digital Information.

1.6 All connected assets must be verified as free from malware or other security risks.

1.7 Company Digital Assets must be physically and digitally secured at all times using appropriate safeguards such as locking devices, controlled access, and encryption.

1.8 Only Company-approved removable media may be used, and it must be encrypted when storing or transporting Company Digital Information.

1.9 Team Members may use the Company's Digital Assets and Accounts for limited and reasonable personal use which is:

a) infrequent;

b) cost-free;

c) non-disruptive to their duties; and

d) does not negatively affect others, Company operations, reputation, or cybersecurity.

1.10 The Company, its authorized Contractors and government agencies may monitor and inspect without notice all content Personnel and Excluded Contractors view, create, receive, or transmit using South Bow's Digital Assets or Accounts.

1.11 South Bow does not guarantee the maintenance, security, privacy, or recovery of personal Digital Information (e.g., contacts, photos, voicemail, documentation, email) on the Company's Digital Assets.

2 Use of non-South Bow Digital Assets

2.1 Personal non-South Bow Digital Assets may connect to Company networks only via the guest network, unless specifically authorized by a legal agreement.

2.2 The Company does not assume responsibility for the security of personal or non-Company assets.

2.3 Personal devices may only connect to the designated SOBO-Guest network. The guest network SSID and password are posted **only on printed signage** located inside designated conference rooms. No exceptions or waivers are permitted.

2.4 All unauthorized connections to Company networks are prohibited.

3 Cybersecurity Incidents

3.1 All suspected or confirmed Cybersecurity Incidents involving South Bow's Digital Assets or Digital Information must be reported immediately, either by calling the Service Desk at 1-877-366-4332 in Canada and the U.S. or submitting a ticket through the ServiceNow support portal.

4 Cybersecurity awareness

4.1 All Team Members must complete the cybersecurity awareness training assigned by the CSO.

4.2 All Team Members and Excluded Contractors must exercise due diligence, detecting, avoiding, and reporting Social Engineering cyber-attacks, such as phishing, when using South Bow's Digital Assets. Reporting of Social Engineering attempts can be done through Microsoft Outlook's Report-a-Phish icon or, when urgent, by calling the Service Desk at 1-877-366-4332. Individuals who do not exercise due diligence regarding Social Engineering cyber-attacks will be subject to disciplinary actions such as having certain access or privileges revoked.

5 Digital Asset and Digital Information management

5.1 All Digital Assets and Information must be accurately inventoried, continuously available, clearly assigned to a Digital Asset or Digital Information Owner and aligned with the expectations of the CSO and the Information Management Policy.

5.2 Access to Digital Assets and Information must be limited to authorized Personnel based on the Principle of Least Privilege, with regular review to ensure continued compliance.

6 Nonconformance reporting

6.1 In addition to the reporting requirements described in the Your Responsibility section of this Policy, Information Owners, Digital Asset Owners and their authorized Employees and Contractors with cybersecurity responsibilities must also report all known non-conformances with this Policy using the South Bow Nonconformance Management Process.

Your responsibility

Team Members and Excluded Contractors must follow all applicable provisions and the spirit and intent of this Policy and support others in doing so. You must promptly report any suspected or actual violation of this Policy through available channels so that South Bow can investigate and address it appropriately. Those who violate this Policy or knowingly permit others under their supervision to violate it may be subject to appropriate corrective action, up to and including termination of employment or contract, as applicable, in accordance with the Company's corporate governance documents, employment practices, contracts, and agreements.

South Bow supports the reporting of suspected breaches of governance, laws, regulations, health, safety, environmental incidents, and near hits, and takes all reports seriously. Those who report in good faith are protected from retaliation, though this protection does not extend to intentionally false or malicious reports or attempts to shield personal negligence or misconduct.

Interpretation and administration

The Company has sole discretion to interpret, administer and apply this corporate governance document and to change it at any time to address new or changed legal requirements or business circumstances.

Definitions

Artificial Intelligence (AI) refers to the capability of computer systems or software to perform tasks that typically require human intelligence. These tasks may include learning from data, recognizing patterns, making decisions, understanding natural language, and solving problems. AI systems can range from simple rule-based automation to advanced machine learning models that adapt and improve over time. AI includes tools and platforms that assist with data analysis, content generation, forecasting, automation, and decision support, provided they are approved and used in accordance with company policies and applicable laws.

Account means any identity, authentication mechanism or email address used for accessing any Digital Asset.

Company Business means all business activities undertaken by Employees and Contractors during the Company's operations or on the Company's behalf, on or off South Bow's premises.

Contractor means a third party hired by South Bow to perform services for or supply equipment, materials, or goods to the Company. Contractors include, without limitation, Contingent Workforce Contractors and Excluded Contractors.

Contingent Workforce Contractor (CWC) means an individual who:

- is employed by a third party to work on behalf of South Bow;
- uses South Bow's assets (e.g., workstation, email, phone) and corporate services;
- is compensated on an hourly or daily rate basis; and
- works under the direction of a South Bow leader.

Data means facts represented as text, numbers, graphics, images, sound, or video. Data is the raw material used to represent Information, or from which Information is derived.

Digital Asset means any network device, computer system, application, data storage systems, or service (and associated data required for operation). This includes, but is not limited to, laptops, tablets, smartphones, and removable media.

Digital Asset Owner (DAO) means a Vice-President or above accountable for South Bow Digital Asset's risk management, lifecycle management, financial investments, contract management, and compliance with South Bow policies, standards, and applicable legal (including without limitation Cybersecurity and Privacy) requirements. The DAO may assign responsibilities of South Bow Digital Asset to DAO Delegate.

Digital Information means any Information that exists in a digital form.

Employee means full-time, part-time, temporary and student employees of South Bow.

Excluded Contractor means a third party or individual employed by a third party who:

- delivers services, equipment, materials, or goods to the Company using their own tools and assets (e.g., workstation, laptop, email, phone, PPE, vehicle);
- does not increase South Bow corporate headcount and overhead costs;
- does not use South Bow's assets and corporate services; and
- directs their own work or receives direction from their employer.

Cybersecurity Incident means an occurrence that can jeopardize the confidentiality, integrity, or availability of a Digital Asset, or constitutes an imminent threat or violation of this Policy and associated cybersecurity standards.

Information means any content, Data, materials, or document created or received during Company Business, regardless of the source, medium or form (printed or electronic, including instant and text messages). Information may either be a Record or a Transitory Record.

Information Owner means the Personnel designated by the business group to be accountable for the confidentiality, quality, integrity, availability, use and disposition of Information created and used to carry out Company Business.

Inter-Affiliate Rules means, collectively, the Interstate Commerce Act (ICA) and the rules and regulations of the Federal Energy Regulatory Commission in the U.S.; along with the Canadian Energy Regulatory Act in Canada.

Personal Information Personal Information means any information on its own or when combined with other information, which can be used to identify an individual. Personal Information may include but is not limited to: employee number, name, contact information (personal and business addresses, phone numbers and emails), date of birth and age, gender or sex, sexual orientation, race, religious affiliation, ethnic origin, marital or family status, political belief, disability, medical information, health care identification number, biometrics, voice recording, photographs, video, salary, benefits, banking information (credit card and bank accounts), Social Security Number (SSN) or Social Insurance Number (SIN), National Identification Number, licenses (including membership numbers), passport numbers, training records, employment history, resumes, opinions about the person (including references, interview notes, performance appraisals, and succession plans) and identifying remarks, and any similarly sensitive or private information. Personal Information includes Protected Health Information (PHI) and sensitive financial information, which might be subject to enhanced protection and disclosure requirements depending on the jurisdiction. Personal Information excludes Aggregated Information.

Principle of Least Privilege means the practice of restricting access and assignment of privileges based on an individual's job classification, job function, and the person's authority to access specific Digital Assets. It ensures users have an appropriate level of access to and within an application or system.

Record means Information, however recorded or stored, providing evidence of activities performed or considered, and/or decisions made pursuant to legal obligations or in a transaction of Company Business.

Social Engineering means the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

South Bow or the **Company** means South Bow Corporation and its wholly-owned subsidiaries and/or operated entities.

Transitory Record means Information that has short-term value, helps complete a routine Company Business activity or prepares a Record, and is not needed as evidence.

References

Related corporate governance and supporting documents

- Artificial Intelligence (AI) Policy
- Code of Business Ethics Policy
- Cybersecurity Password Standard

- Cybersecurity Standards
- Information Management Policy
- Inter-Affiliate Rules Compliance Manual
- Protection of Personal Information Policy
- South Bow Nonconformance Management Process

How to contact us

- Policy Questions and Comments
- ServiceNow support portal link

South Bow's reporting channels

- Ethics Helpline
- Corporate Compliance
- Human Resources
- Legal department
- Compliance Coordinators