Cargill Global Compliance Policy

Information Protection and Management Policy

SCOPE

This policy applies to users of Cargill technology assets, and those Cargill businesses and functions that rely upon technology resources and information assets for running their business.

PURPOSE

Technology resources and information assets play an important role in the success of our business. They can help us make better and faster decisions. We want to feel confident that the information available to us is accurate and complete. We want our technology resources available to us when we need them. Our plant systems depend upon a reliable, near real-time flow of information to control processes safely and productively. This policy focuses on protecting and managing these resources accordingly.

POLICY REQUIREMENTS

Cargill resources and assets, including those falling into the technology, information, and related process areas, are required to be protected and managed relative to their criticality, confidentiality, and value to Cargill.

Technology resources and information assets are expected to be protected based on an assessment of internal Cargill requirements (policies and standards, whether, and to what extent, there is value or benefit for the Enterprise, Business or Function to expend time and resources to keep the information available and accurate) as well as external requirements such as those conveyed through external sources such as governmental regulation, contractual requirements, and other obligations. Controls must be suitable given the reasonable value of, and risks to, information assets based on how/where information is used.

To support the management and protection of our technology resources and information assets, Cargill will:

- Manage the technology risk incurred as a result of our relationships with external parties.
- Ensure that businesses and functions have appropriate plans in place to respond to disruptions or incidents that take into account the management of staff welfare issues, media communication, and liaising with appropriate emergency services.
- Provide access to Cargill technology and information assets at the level required to meet an approved business need or to perform prescribed job responsibilities.
- Maintain a global information protection awareness and training program.

Owners of information assets are:

- Accountable for knowledgably understanding and assessing information and technology risks and ensuring appropriate protections are prescribed.

Users of technology resources and information assets must:

- Properly manage physical and logical access methods, such as IDs and passwords.
- Report and manage security incidents and violations appropriately and in a timely manner.
- Take reasonable steps to preserve the integrity, availability and disclosure of these resources and assets in alignment with the information owner, business need and operational processes.

Failure to comply with this policy and its procedures may lead to disciplinary action, up to and including termination.

RELATED PROCEDURES

The following procedures are user oriented, and apply to users of Cargill technology assets:

- IDs and Passwords
- Incident Reporting
- Information Access

The following procedures are business oriented, and apply to those Cargill businesses and functions that rely upon technology resources and information assets for running their business:

- Data Backup
- Information Protection Awareness and Training
- Joint Venture
- Resiliency Management
- Third Parties

ADDITIONAL REFERENCES

This policy supports the following Cargill Guiding Principles:

- #1: We obey the law.
- #6: We protect Cargill's information, assets and interests.

Confidential Information Policy (and its Procedures)

Data First:

- Data First helps you make informed and consistent choices about how to protect your most important data.
- Data First guidance and support documents, including information protection models, data categories, definitions and examples, are available here.

Physical access protections:

- Physical access protections are one layer of a "defense in depth" approach designed to protect technology and information assets. Refer to Cargill's "Physical Security Policy" for requirements and guidance on protecting technology and information assets from unauthorized physical access.

POLICY OWNER / VERSION

Global IT

Technology Governance, Risk and Control

2/7/2019