

	<b>PUBLIC</b>	<b>INTERNAL USE</b>	<b>CONFIDENTIAL</b>	<b>RESTRICTED</b>
<i><b>Risk Level</b></i>	None	Routine	Moderate	Greatest
<i><b>Sensitivity Level</b></i>	Open or unclassified	Low – Medium	Moderate - High	High - Critical
<i><b>Definition</b></i>	<b>PUBLIC</b> information is information that can be disclosed to anyone without violating an individual’s right to privacy. Knowledge of this information does not expose the corporation to financial loss, embarrassment, or jeopardize the security of assets.	<b>INTERNAL USE</b> information is information that, due to technical or business sensitivity, is limited to employees and contractor who work on-site. It is intended for use only within the corporation. Unauthorized disclosure, compromise, or destruction would not have a significant impact on the corporation or its employees.	<b>CONFIDENTIAL</b> information is information that the corporation and its employees have a legal, regulatory, or social obligation to protect. It is intended for use solely within defined groups in the corporation. Unauthorized disclosure, compromise, or destruction would adversely impact the corporation or its employees.	<b>RESTRICTED</b> information, the highest level of classification, is information whose unauthorized disclosure, compromise, or destruction could result in severe damage, provide significant advantage to a competitor, or incur serious financial impact to the corporation or its employees. It is intended solely for restricted use within the corporation and is limited to those with an explicit, predetermined “need to know.”
<i><b>Examples</b></i>	<ul style="list-style-type: none"> <li>• Marketing brochures</li> <li>• Customer disclosure statements</li> <li>• Published annual reports</li> <li>• Interviews with news media</li> <li>• Press releases</li> </ul>	<ul style="list-style-type: none"> <li>• Employee Handbook</li> <li>• Telephone Directory</li> <li>• Organization Charts</li> <li>• Policies and Standards</li> </ul>	<ul style="list-style-type: none"> <li>• Personnel records</li> <li>• Customer records</li> <li>• Unit business plans</li> <li>• Correspondence containing customer information</li> <li>• Proprietary/custom software</li> <li>• Budget information</li> </ul>	<ul style="list-style-type: none"> <li>• Strategic Plans</li> <li>• Online access codes such as passwords or pins</li> <li>• Credit card listings</li> <li>• Encryption keys</li> </ul>

**Information Asset Classification Matrix**

### ***Responsibilities***

To facilitate the protection of information, employee responsibilities have been established at three levels: **Owner, Custodian** and **User**.

- **Owner:** Is the management of an organizational unit, department, etc. where the information is created, or that is the primary user of the information. Owner in this case means the employee responsible for the information assets. Company retains actual legal ‘ownership’ of information assets.  
Owners are responsible to:
  - identify the classification level of all information within their organizational unit,
  - define and implement appropriate safeguards to ensure the confidentiality, integrity, and availability of the information resource,
  - assessing and monitoring safeguards to ensure their compliance and report situations of non-compliance,
  - authorize access to those who have a business need for the information, and
  - ensure access is removed from those who no longer have a business need for the information.
- **Custodian:** Employees designated by the Owner to be responsible for maintaining the safeguards established by the Owner.
- **User:** Employees authorized by the Owner to access information and use the safeguards established by the Owner. Being granted access to information does not imply or confer authority to grant other users access to that information.

### ***Misuse of Company Data***

Misuse of Company data may result in disciplinary action, up to and including dismissal.

Employees are not to divulge, use, or make information about the Company's employees or customers available to anyone outside the Company or between affiliate organizations.. This prohibition includes mailing lists, names, addresses, telephone numbers, and any records of a financial or energy consumption nature. Employees should refer all requests for this type of information, or any similar appearing information, to their supervisors.

**Note:** Employees may release information to individuals about their own homes or businesses.

Employees specified by local management will handle employment verification or other related information concerning past or present employees.

***Destruction of Sensitive Records***

The National Association of Regulatory Utility Commissioners (NARUC) regulations state that employees should take precautions to destroy the legibility of records for which the content is forbidden by law to be divulged to unauthorized persons. If you have any question regarding the confidentiality of data, contact the Document Control Center (DCC) for assistance.

Destroy any duplicate records and work papers of a sensitive or confidential nature by shredding or other appropriate methods. Never place sensitive or confidential data in the trash.