

# Information Classification Policy

(ISO/IEC 27001:2005 A.7.2.1)

COMPANY provides fast, efficient, and cost-effective electronic services for a variety of clients worldwide. As an industry leader, it is critical for COMPANY to set the standard for the protection of information assets from unauthorized access and compromise or disclosure. Accordingly, COMPANAY has adopted this information classification policy to help manage and protect its information assets.

**All COMPANY associates share in the responsibility for ensuring that COMPANY information assets receive an appropriate level of protection by observing this Information Classification policy:**

- Company Managers or information ‘owners’ shall be responsible for assigning classifications to information assets according to the standard information classification system presented below. (‘Owners’ have approved management responsibility. ‘Owners’ do not have property rights.)
- Where practicable, the information category shall be embedded in the information itself.
- All Company associates shall be guided by the information category in their security-related handling of Company information.

All Company information and all information entrusted to Company from third parties falls into one of four classifications in the table below, presented in order of increasing sensitivity.

Information Category	Description	Examples
Unclassified Public	Information is not confidential and can be made public without any implications for Company. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	<ul style="list-style-type: none"> <li>• Product brochures widely distributed</li> <li>• Information widely available in the public domain, including publicly available Company web site areas</li> <li>• Sample downloads of Company software that is for sale</li> <li>• Financial reports required by regulatory authorities</li> <li>• Newsletters for external transmission</li> </ul>
Proprietary	Information is restricted to management-approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	<ul style="list-style-type: none"> <li>• Passwords and information on corporate security procedures</li> <li>• Know-how used to process client information</li> <li>• Standard Operating Procedures used in all parts of Company's business</li> <li>• All Company-developed software code, whether used internally or sold to clients</li> </ul>
Client Confidential Data	Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	<ul style="list-style-type: none"> <li>• Client media</li> <li>• Electronic transmissions from clients</li> <li>• Product information generated for the client by Company production activities as specified by the client</li> </ul>
Company Confidential Data	Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	<ul style="list-style-type: none"> <li>• Salaries and other personnel data</li> <li>• Accounting data and internal financial reports</li> <li>• Confidential customer business data and confidential contracts</li> <li>• Non disclosure agreements with clients\vendors</li> <li>• Company business plans</li> </ul>

**Manager  
Manager Title  
9 July 2008**