# LeMoyne-Owen College Data Classification Policy

LeMoyne-Owen College (LOC) provides a transformative experience educating students for urban-focused leadership, scholarship, service and professional careers. As an industry leader, it is critical for LOC to set the standard for the protection of information assets from unauthorized access and compromise or disclosure. Accordingly, LOC has adopted this information classification policy to help manage and protect its information assets.

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

- LOC 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 LOC associates shall be guided by the information category in their security-related handling of LOC information.

All LOC information and all information entrusted to LOC 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 LOC. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital. | • Product brochures widely distributed<br>• Information widely available in the public domain, including publicly available LOC web site areas<br>• Financial reports required by regulatory authorities<br>• Newsletters for external transmission |
| Proprietary | Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence LOC'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. | • Passwords and information on corporate security procedures<br>• Know-how used to process client information<br>• Standard Operating Procedures used in all parts of Company's business<br>• All LOC-developed software code, whether used internally or sold to clients |
| Client Confidential | Information received from clients in any form for processing in production by | • Client media<br>• Electronic transmissions from |

| | | |
|---|---|---|
| Data | LOC. 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. | clients<br>• Product information generated for the client by LOC production activities as specified by the client |
| Company Confidential Data | Information collected and used by LOC 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 LOC. The highest possible levels of integrity, confidentiality, and restricted availability are vital. | • Salaries and other personnel data Accounting data and internal financial reports<br>• Confidential customer business data and confidential contracts<br>• Non-disclosure agreements with clients\vendors regarding LOC business plans |