![phonovation - Power to Interact]

Quality Control & Compliance Initiative

DATA CLASSIFICATION POLICY

Author:	**Phonovation Quality Control Group**
	Gavin Carpenter
Effective Date:	12th Nov 2013
Revised:	20th Jan 2015
Revised by:	Pedro Quintas
To:	All Phonovation Staff

This document is publicly available to any staff member on the following network path:

File:\\srvadmdc00\dev & it\Quality Control\QC - Phonovation Data Classification Policy.docx

Data Classification Policy

Phonovation provides fast, efficient, and cost-effective electronic services for a variety of clients worldwide.

As an industry leader, it is critical for Phonovation to set the standard for the protection of information assets from unauthorized access and compromise or disclosure. Accordingly, Phonovation has adopted this information classification policy to help manage and protect its information assets.

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

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

All Phonovation information and all information entrusted to Phonovation 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 Phonovation. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	• Product brochures widely distributed • Information widely available in the public domain, including publicly available Phonovation web site areas • Sample downloads of Phonovation software that is for sale • Financial reports required by regulatory authorities • Newsletters for external transmission
Proprietary	Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence Phonovation'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 • Know-how used to process client information • Standard Operating Procedures used in all parts of Phonovation's business • All Phonovation-developed software code, whether used internally or sold to clients
Client Confidential Data	Information received from clients in any form for processing in production by Phonovation. 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.	• Client media • Electronic transmissions from clients • Product information generated for the client by Phonovation production activities as specified by the client
Company Confidential Data	Information collected and used by Phonovation in the conduct of its business to employ people, to log and fulfil 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.	• Salaries and other personnel data • Accounting data and internal financial reports • Confidential customer business data and confidential contracts • Non-disclosure agreements with clients\vendors • Phonovation business plans