# 1.People Information Classification Policy

| Change | Date | Version |
|---|---|---|
| Introduced | November 2013 | 1.00 |
| | | |
| | | |

## 2. Introduction

People provides fast, efficient, and cost-effective HR services for a variety of clients worldwide. It is critical for People to set the standard for the protection of information assets from unauthorized access and compromise or disclosure. Accordingly, People has adopted this information classification policy to help manage and protect its information assets.

All People associates share in the responsibility for ensuring that People 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.

# 3. Classifications

| Information Category | Description | Details |
|---|---|---|
| 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. | Documents in the public domain available from our website, our support desk and our social media channels.<br><br>Examples include:<br>• Product brochures widely distributed<br>• Information widely available in the public domain,<br>including publicly available Company web site areas<br>• Sample downloads of Company software that is for<br>sale<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 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. | • 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 Company-developed software code, whether used internally or sold to clients<br>Client Confidential Data |

| | | |
|---|---|---|
| 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. | • Client HR data<br>• All customer account data including sales data and accounts and account management<br>• All help desk data on client calls and any specific communication to clients |
| 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. | • Salaries and other personnel data<br>• Accounting data and internal financial reports<br>• Confidential customer business data and confidential contracts<br>• Non disclosure agreements with clients \vendors<br>• Company business plans |