

A8 - INFORMATION CLASSIFICATION MATRIX AND HANDLING GUIDE

CATEGORY	DESCRIPTION	SAMPLE DOCUMENTS	MARKING	ADMIN CONTROLS	STORAGE	REPRODUCTION	DISTRIBUTION	DESTRUCTION/ DISPOSAL
UNCLASSIFIED / PUBLIC	Information is not confidential and can be made public without any implications for Digicall Group. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	<ul style="list-style-type: none"> * Product brochures widely distributed. * Information widely available in the public domain, including publicly available Digicall Group web site areas. * Sample downloads of Digicall Group software that is for sale. * Financial reports required by regulatory authorities. * Newsletters for external transmission 	None	None	No Requirements	Unlimited	No restrictions	Recycling/General Waste
PROPRIETARY	Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence Digicall Group'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"> * Passwords and information on corporate security procedures. * Know-how used to process client information. * Standard Operating Procedures used in all parts of Digicall Group business. * All Digicall Group developed software code, whether used internally or sold to clients. 	<p>"INTERNAL USE ONLY"</p> <p>Paper Documents: Apply to bottom centre of each page.</p> <p>Other Media: Label across the media.</p>	<p>Author: responsible for proper markings.</p> <p>User: responsible for proper storage and document control.</p>	<p>Encryption: Does not require encryption</p> <p>Paper documents: No physical protection requirement</p> <p>Electronic data: No protection required</p>	Limited copies may be made only by employees, or by contractors and third parties who have signed an appropriate nondisclosure agreement.	<p>Internal: use an internal mail envelope.</p> <p>External: use a sealed envelope.</p> <p>Electronic: use internal email system. Encryption is required for transmission to external email addresses.</p>	<p>Paper documents: shred.</p> <p>Electronic data: erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal</p>
CLIENT CONFIDENTIAL DATA	Information received from clients in any form for processing in production by Digicall Group. 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"> * Client media. * Electronic transmissions from clients. * Product information generated for the client by Digicall Group production activities as specified by the client. 	<p>"CLIENT CONFIDENTIAL"</p> <p>Paper Documents: Apply to bottom centre of each page.</p> <p>Other Media: Label across the media</p>	<p>Originator: responsible for ensuring that confidential information is distributed on a strict need-to-know basis.</p> <p>Recipient: responsible for ensuring that confidential information is encrypted and/or kept under lock & key when not in use.</p>	<p>Encryption: Must be encrypted during storage.</p> <p>Paper documents: Must not be printed without approval of owner. Must be stored in a locked cabinet when not in use.</p> <p>Electronic data: Should be stored in a protected electronic folder and access to the folder should be auditable.</p>	None	<p>Internal: use a sealed envelope inside an internal mail envelope. Hand deliver if possible.</p> <p>External: use a plain sealed envelope. Hand deliver or send by registered mail, courier <i>etc.</i></p> <p>Electronic: Email - Encrypt data. File Transfer - use Secure protocols (SFTP)</p>	<p>Paper documents: shred using an approved cross-cut shredder.</p> <p>Electronic data: erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal.</p>
COMPANY CONFIDENTIAL DATA	Information collected and used by Digicall Group 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 Digicall Group. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	<ul style="list-style-type: none"> * Client media. * Salaries and other personnel data. * Accounting data and internal financial reports. * Confidential customer business data and confidential contracts. * Non-disclosure agreements with clients/vendors. * Digicall Group business plans. 	<p>"COMPANY CONFIDENTIAL"</p> <p>Paper Documents: Apply to bottom centre of each page.</p> <p>Other Media: Label across the media</p>	<p>Originator: responsible for ensuring that confidential information is distributed on a strict need-to-know basis.</p> <p>Recipient: responsible for ensuring that confidential information is encrypted and/or kept under lock & key when not in use.</p>	<p>Encryption: Must be encrypted during storage.</p> <p>Paper documents: Must not be printed without approval of owner. Must be stored in a locked cabinet when not in use.</p> <p>Electronic data: Should be stored in a protected electronic folder and access to the folder should be auditable.</p>	None	<p>Internal: use a sealed envelope inside an internal mail envelope. Hand deliver if possible.</p> <p>External: use a plain sealed envelope. Hand deliver or send by registered mail, courier <i>etc.</i></p> <p>Electronic: Email - Encrypt data. File Transfer - use Secure protocols (SFTP)</p>	<p>Paper documents: shred using an approved cross-cut shredder.</p> <p>Electronic data: erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal.</p>