

Information Classification Guide

Information Category	Description	Example Documents	Marking	Administrative Controls	Reproduction Controls	Handling Instructions	Disposal Rules
PUBLIC	Information that may be widely distributed without causing financial or reputational damage to the company, its employees and / or shareholders.	Marketing materials such as PR releases, brochures etc.	“FOR PUBLIC USE” Apply to top and bottom centre of each page	The document author is responsible for ensuring the document is properly marked.	No controls	Documents MAY be sent outside the company without authorisation. Documents MAY be stored online. Documents MAY be emailed over the internet.	Recycle as appropriate.
INTERNAL	Information which, if disclosed without authorisation, would be inconvenient to the organisation, its employees and / or shareholders. Authorisation may be granted by the data Author or a company Manager.	Most corporate information. Company internal memos, minutes, training materials, work instructions, contact directories, productivity reports, Service Level Agreements, negotiation briefings, Intranet Pages	“INTERNAL USE ONLY” Apply to top and bottom centre of each page	The document author is responsible for ensuring the document is properly marked. Recipients of documents are responsible for proper storage and control.	Copies may only be made by company employees or contractors / 3 rd parties where a non-disclosure agreement is in place.	Documents MUST NOT be sent outside the company without authorisation. Documents MAY be sent in internal mail. Documents MAY be sent by external mail but MUST use a sealed envelope. Documents MAY be sent by email to other employees over the corporate email system. Documents MAY only be sent to non-company email addresses with authorisation. Documents MAY be faxed to other company locations or to other numbers with authorisation.	Must be sent for disposal using company approved methods.
CONFIDENTIAL	Sensitive or valuable information, including proprietary and research data. Release of this information may affect company share prices or adversely reflect on the company or its employees. This information must not be disclosed without authorisation from a Director or their deputy.	All data relating to company plans and developments. Such as R&D data, transaction data, productivity reports, project initiation documents, audit reports, contracts, accounting data, planned mergers & divestitures.	“CONFIDENTIAL” Apply to top and bottom centre of each page	The Author is responsible for ensuring the document is properly marked and is only distributed to people who have a genuine need to know the data. Recipients are responsible for ensuring the data is properly accounted for while in their possession. Printed copies must be stored in locked containers when not in use.	Copies may only be made by the Author or with the written permission of a Director or deputy. A record of copies must be maintained.	Data may not be sent outside the company without Director authorisation. Documents MAY be sent by internal mail but must be in a sealed envelope. Documents MAY be sent by external mail but must use a registered / recorded delivery method. Documents must be encrypted if sent over email. Encryption keys (passwords) must be sent separately. Documents MAY be sent by fax but must require phone confirmation prior to sending and confirmation of full receipt.	Paper documents MUST be shredded before being sent for disposal. Electronic data MUST be wiped before being sent for disposal. Disposal is through normal company channels.

Information Category	Description	Example Documents	Marking	Administrative Controls	Reproduction Controls	Handling Instructions	Disposal Rules
SENSITIVE	<p>Information which is controlled by a regulatory agency or is of a nature which will affect share price if released into the public domain.</p> <p>This information must not be disclosed without the authorisation of two Directors (not deputies).</p> <p>Access to this data is only permitted to employees and shareholders who have a valid business need and are included on the Critical Induction Register.</p>	<p>Any data with personal information or relating to Key Financial Systems. Any data which is subject to regulatory (e.g. FSA) inspection.</p> <p>This includes HR records, disciplinary records, performance reviews, investment strategies, profit projections (before release) etc.</p>	<p>“COMMERCIAL – SENSITIVE”</p> <p>Apply to top and bottom centre of each page.</p>	<p>The Author is responsible for ensuring the document is properly marked and ONLY sent to people who are on the Critical Induction Register.</p> <p>Recipients are responsible for ensuring the data is properly protected at all times and MUST NOT permit this data to go outside the induction list.</p>	<p>Copies may only be made by the Author or with the written permission of two Directors.</p> <p>Copies may only be made on approved devices.</p> <p>A record of copies must be maintained.</p>	<p>Data MUST NOT be sent to anyone not on the Critical Induction Register.</p> <p>Data MAY NOT be sent over internal mail but MAY be hand delivered by the Author.</p> <p>Data MAY be sent externally using double enveloping and registered / recorded delivery.</p> <p>Data MUST be encrypted when sent electronically. Encryption keys (passwords) must be sent separately.</p> <p>Data MAY NOT be sent by fax.</p>	<p>Paper documents MUST be shredded using the dedicated shredder before being sent for disposal.</p> <p>Electronic data MUST be securely erased using a Company approved process before being sent for disposal.</p> <p>Disposal is through normal company channels.</p>

Provided by

Halkyn Consulting Ltd

Specialist Security Consultants

For more information on how we can help you improve your security, visit us on the web at www.halkynconsulting.co.uk or send an email to info@halkynconsulting.co.uk and we will be in touch to discuss your needs.

As a fully independent consultancy, we are able to assess what measures best suit your requirements from a range of vendors to ensure that you get cost-effective security that fits your business.

We are experienced in advising and assisting all size of business protect their assets, reassure their customers and win new contracts based on their enhanced security posture.

Using SC cleared consultants with internationally recognised qualifications we are able to assess your security against a range of standards and work with our clients to ensure that the most suitable ones are applied.

Based in North Wales, we are able to work with clients anywhere in the world and, through on-site visits and assessments we ensure that all our advice is based on realistic, credible, threat assessments based on the local situation.

Our services will help your business grow, win new business and protect its assets and reputation in a changing world. Get in touch today.