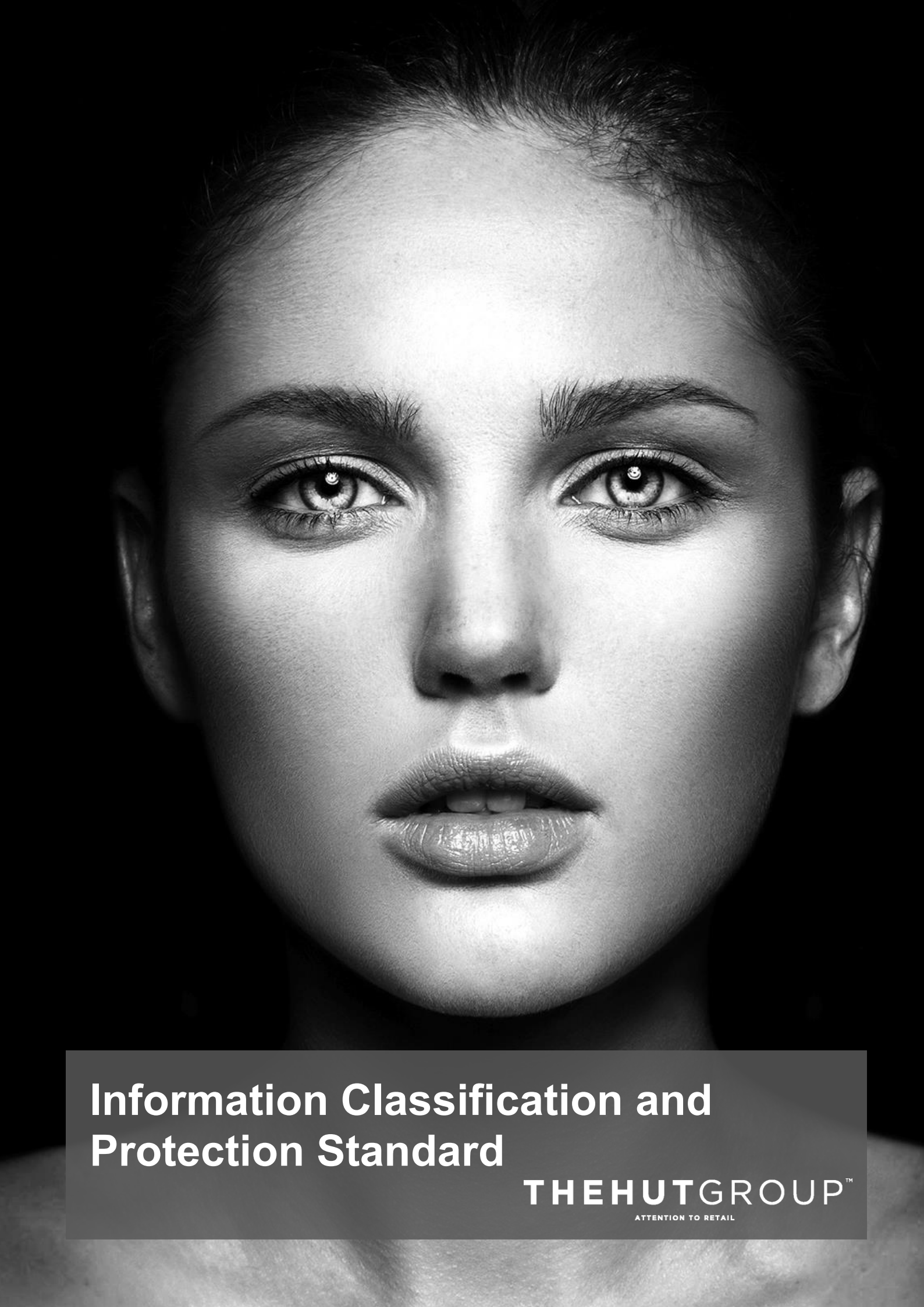

Information Classification and Protection Standard

THEHUTGROUP™

ATTENTION TO RETAIL

Version: v1.0
Effective: March 2016
Owner: Graham Thomson, Chief Information Security Officer

Version History:

Version	Author	Description	Reason for Amendment	Date	Next review
1.0	Peter Stanfield	New live standard	New live standard	March 2016	March 2017

Contents

1. Introduction

The Hut Group has a regulatory and legal responsibility to classify and protect its information.

This document details the mandatory requirements that The Hut Group has set for classifying and protecting its information. It applies to all The Hut Group business units, operations, functions, and staff, including permanent and temporary employees and third-party personnel such as agents, temporaries, contractors, and consultants, who have access to The Hut Group information, herein referred to as Staff.

Failure to protect certain types of information adequately could lead to a serious loss or breach which in turn could result in a significant financial penalty against us, a serious loss of customer confidence, and/or critical damage to The Hut Group's reputation.

To protect against these risks this document must be read and followed by all Staff. We are all responsible for protecting the information we work with and we must take these obligations seriously.

Any employee found to have violated the requirements of this standard may be subject to disciplinary action, up to and including termination of employment.

2. What is information classification?

In order to indicate how sensitive a piece of information is it is given a grading (a classification). From this grading the appropriate protective measures can be identified. All The Hut Group information must be classified as one of the following:

- **PUBLIC** (***non-sensitive, anyone can access it***)
- **INTERNAL** (***mildly sensitive, basic protection required***)
- **CONFIDENTIAL** (***very sensitive, special security requirements apply***)

Overall, information must be classified at the **level of its highest component part**.
For example, if a document contains four pages of INTERNAL and only one page of CONFIDENTIAL information, then the whole document is classified as CONFIDENTIAL.

3. What are the definitions of each classification?

When classifying information, imagine what would happen if the information you're handling landed in the wrong hands (such as the media, a competitor, or a criminal), or was maliciously altered or deleted (and was not backed up). The more serious the damage caused to our business, the higher the classification should be.

The Hut Group information classifications and their definitions are:

- **PUBLIC**
  - **Definition**: non-sensitive information approved for external (i.e. public) release
  - **Risk from unauthorised disclosure/use**: no impact or damage caused
  - **Security requirements**: none, but PUBLIC information must be reviewed and authorised by the appropriate senior managers before its release to the public
  - **Examples**:
    - ✓ Information on our publicly available websites
    - ✓ Advertising or public news articles
    - ✓ Corporate statements to the media
    - ✓ Published annual reports
- **INTERNAL**
  - **Definition**: information that is **private** to The Hut Group personnel (whether for all staff, defined functions or individuals) and authorised external parties only
  - **Risk from unauthorised disclosure/use**: a minor impact to The Hut Group (i.e. a small but tolerable financial, operational or reputational impact)
  - **Security requirements**: basic, common sense security measures need to be applied to ensure that access to it is limited to those who need to know
  - **Examples**:
    - ✓ THG Wiki content
    - ✓ Staff business communications (e.g. non sensitive, day to day emails)
    - ✓ General office documents, such as policies and procedures
    - ✓ Staff objectives
    - ✓ Staff telephone listings and other internal contact information

- **CONFIDENTIAL**
  - **Definition**: information that is **highly sensitive** to The Hut Group, or is required by law(s) or regulation(s) to be protected appropriately
  - **Risk from unauthorised disclosure/use**: a serious impact to The Hut Group (i.e. a large financial impact, a serious reduction in operational capability, or a serious reputational impact that would damage The Hut Group in the long term)
  - **Security requirements**: special, specific security measures need to be applied to ensure the information is protected from unauthorised access, modification or deletion
  - **Examples**:
    - ✓ Payment card data, such as full credit card numbers (protection required by the Payment Card regulator)
    - ✓ Personal information that identifies a living person (protection required by the UK Data Protection Act)
      - This flowchart can be used to assess if data is 'personal data': https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf
    - ✓ Sensitive personal information relating to an identifiable living person (protection required by the Data Protection Act):
      - racial or ethnic origin
      - political opinions
      - religious beliefs
      - membership of a trade union
      - physical or mental health or condition
      - sexual life
      - details of alleged or actual criminal offences
      - details of any proceedings for alleged or actual criminal offences
    - ✓ HR staff information
    - ✓ Legal or contractual data involving 3rd parties
    - ✓ New product information, until approved for disclosure
    - ✓ Mergers and acquisitions details, until approved for disclosure
    - ✓ Passwords to The Hut Group's IT systems
    - ✓ Sensitive technology information, including propriety source code
    - ✓ Trade secrets (e.g. the recipe for MyProtein items, etc)

4. Responsibilities: who are information owners?

Ultimately all information we create, store and/or process is legally owned by The Hut Group.

However, each of us is responsible for ensuring that the information we handle is classified properly, stored securely to prevent unauthorised access, securely transferred whether electronically or by courier/post, and disposed of appropriately. Hence, we are all information owners.

5. How should I mark my information with its classification?

In order to make others immediately aware that a document is sensitive all CONFIDENTIAL information must be marked. To do this mark the word CONFIDENTIAL within the footer of the documentation.

The default classification for all information is INTERNAL and there is no requirement to mark information in this category.

There is no requirement to mark information classified as PUBLIC.

6. Working away from the office

When handling ANY company information outside of the office ensure that you take precautions to protect it from loss, theft and unauthorised access.

When working on CONFIDENTIAL information ensure it cannot be overlooked or overheard when working in public places (e.g. trains, airports, hotels, etc).

Always securely dispose of CONFIDENTIAL information – **do NOT use paper recycling or waste bins**. If no secure disposal is available, keep it secured and take it back to the office to dispose of securely later.

CONFIDENTIAL information must NEVER be worked on from a public computer (e.g. internet cafes).

7. Physical transportation

Information and technical assets must be protected against the risks of loss, theft and unauthorized access during physical transportation away from secure buildings (i.e. moving assets to and from office locations and data centres or third party locations).

Staff transporting information and technical assets must be authorised to do so by the asset owner.

During transportation that assets must be physically protected from the risks of loss, theft and unauthorized access.

Examples of protections include but are not limited to:

- Ensuring only approved and secure couriers are used.
- Physically locking the assets in containers during transportation.
- Assets are inventoried, signed out at one end and signed in at the final location.
- Where possible encryption of devices holding data must be used, i.e. laptops, usb drives etc...
- Assets must never be left unattended unless physically secured and out of sight from potential thieves.

Contact the information security team for advice if in any doubt of how to protect assets.

8. How do I report an information loss or a data breach?

Losses: All losses and thefts of any IT equipment (e.g. laptop or smartphone) must be reported to the Service Desk immediately.

Data Breaches: You must report any breaches of data protection to the Information Security Team via the 'information.security@thehutgroup.com' email address. Provide as much information as possible about the nature of the breach, its scope (e.g. how many customers may have been affected), its cause (if known) and any action already taken to resolve the issue.

Examples of data protection breaches include but are not limited to:

- Loss or theft of a removable media device (e.g. a USB memory stick or CD) containing CONFIDENTIAL information regardless of whether it was encrypted or not.
- Posting/couriering CONFIDENTIAL information to the wrong address or it fails to arrive.
- Emailing CONFIDENTIAL information to the wrong address.

9. How do I securely dispose of my information and technical assets?

- ✓ CONFIDENTIAL paper information must be shredded or deposited in to the secure consoles.
- ✓ CDs & DVDs containing CONFIDENTIAL data can be put through the CD slot on the shredders or handed in to Service Desk.
- ✓ PCs, laptops, & smartphone assets for members of staff that have left the business or that have become redundant must be taken to the Service Desk who will follow the procedure to securely wipe for reassignment or take the steps necessary to dispose of it securely.

10. Where can I find further help and information?

This Standard is owned by the Chief Information Security Officer and all questions or queries regarding it should be directed to the information security team via the team email:

- information.security@thehutgroup.com

ANNEX A - Information Classification and Protection Requirements Table

<table>
<tr><th>Classification</th><th>Storage (e.g. cupboards/file shares/CDs)</th><th>Transfer (e.g. post/courier/email/FTP)</th><th>Disposal</th></tr>
<tr><td>CONFIDENTIAL
very sensitive, special security required
Examples:
-Payment card data (PANs) *see Annex B
-Customer information (e.g. name & phone no)
-Sensitive personal information (as per DPA)
-HR staff information
-Legal and Contractual data involving 3rd parties
-New products, until approved for disclosure
-Mergers and acquisitions, until approved for disclosure
-Passwords
-Source code
-Trade secrets</td><td>As INTERNAL plus:
✓ Mark docs/emails with ‘CONFIDENTIAL’
✓ Grant access on a ‘need to know’ basis
✓ Lock paper documents away when not in use
✓ Do not create documents/emails with full payment card numbers (*see Annex B for details). Only store payment card numbers using the IT systems approved for that purpose
✓ Do not write down payment card details. Only process payment card numbers using the systems approved for that purpose</td><td>As INTERNAL plus:
✓ Do not email full payment card data (e.g. credit card numbers) and only process payment card numbers using the systems approved for that purpose
✓ Use secure file transfer tools to send files
✓ Encrypt external emails / attachments and file transfers (excluding emails to single customers)
✓ Ensure a non-disclosure agreement is in place with Third Parties
✓ Make external recipients aware of any handling instructions
✓ Enclose paper docs in a sealed envelope that prevents sensitive data from being viewed when posting
✓ Confirm receipt of bulk paper distributions</td><td rowspan="2">Paper:
✓ Shred documents, or
✓ Use confidential waste bins
✓ Report losses or thefts to Information Security

Electronic Media:
✓ Take to Service Desk for secure disposal
✓ Report losses or thefts to Service Desk</td></tr>
<tr><td>INTERNAL
mildly sensitive, basic protection required
Examples:
-Internal Wiki sites
-Staff communications
-General office documents
-Staff objectives
-Staff telephone listings</td><td>✓ Store digital files in appropriate folders with access restricted to those who ‘need to know’
✓ Do not use unapproved online file storage services (e.g. OneDrive, Dropbox, Google Docs)
✓ Screen-lock unattended computers
✓ Secure information and technical assets when working away from the offices
✓ Only store information on encrypted removable media (e.g. USB sticks)</td><td>✓ Only use The Hut Group email accounts to send company email (i.e. don’t use personal accounts)
✓ Only use approved file transfer tools to send files
✓ Only send information to recipients who ‘need to know’
✓ Technical assets must be protected against the risks of loss, theft and unauthorized access during physical transportation
✓ Asset owners must approve the transportation of their assets and ensure secure transportation</td></tr>
<tr><td>PUBLIC
non-sensitive, anyone can access it
Examples:
-Information on our publicly available websites
-Advertising or public news articles
-Corporate statements to the media
-Published annual reports</td><td colspan="3">✓ PUBLIC information must be reviewed and authorised by the appropriate senior manager(s) before its release
✓ There are NO security requirements for the storage, transmission or destruction of PUBLIC information</td></tr>
</table>

ANNEX B - Requirements for Storing Payment Card Data

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. It aims to reduce the risk of fraud from data losses or thefts. Failure to protect card data can lead to penalties and very large fines (not to mention the reputational damage that would be caused by any media coverage of the incident).

The Primary Account Number (PAN) is the defining factor in the applicability of PCI DSS requirements.

If the full PAN is ***NOT*** stored, processed, or transmitted, then the PCI DSS requirements ***do not apply*** (because without the full PAN data a fraud cannot be committed on the card).

Data	Data Element	Storage Permitted	Protection Required	Make the data unreadable if stored 4
Cardholder Data	Primary Account Number	Yes	Yes	Yes
	Cardholder Name 1	Yes	Yes 2	No
	Service Code 1	Yes	Yes 2	No
	Expiration Date 1	Yes	Yes 2	No
Sensitive Authentication Data 2	Full Magnetic Stripe Data 3	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

1. These data elements must be protected if stored in conjunction with the PAN. PCI DSS does not apply if full PANs are not stored, processed, or transmitted.
2. Sensitive authentication data **must not be stored after authorisation** (even if encrypted).
3. Full track data from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere.
4. Can be achieved by encryption / hashing / truncation / masking