



Guidelines for Information Labeling and Handling

TRIANZ INTERNAL

trianz.com

Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

Information Classification

| | |
|-------------------------------------|--------------|
| <input type="checkbox"/> | Public |
| <input checked="" type="checkbox"/> | Internal |
| <input type="checkbox"/> | Confidential |
| <input type="checkbox"/> | Restricted |

Table of Contents

| | |
|--|-----------|
| 1. GUIDELINES FOR INFORMATION LABELING AND HANDLING | 4 |
| 2. REFERENCES: | 10 |

1. Guidelines for Information Labeling and Handling

| Control Area | Public | Internal Use Only | Confidential |
|---|--|--|---|
| Access Restrictions | <ul style="list-style-type: none"> □ Accessible to public at large. | <ul style="list-style-type: none"> □ Read access will be granted to all Trianz employees and is solely for internal use □ Employees shall not share information with any third party and/or outsourced employees (unless authorized by departmental head) either by E-mail, hardcopy or verbally | <ul style="list-style-type: none"> □ Access must be limited to named authorized individuals only □ Employees shall not share information with any other person outside his/her own department, third party and/or outsourced employees (unless authorized by departmental head) □ Access by external parties must be subject to a non-disclosure agreement as well as a business need to know □ Any authorized person taking a photocopy of information shall do it personally or get the document photocopied in his own presence. □ While taking out the print of the document the person should collect the print as soon as the print command is executed. □ Handling of information based on the type of Information Asset classification. This will include circulation, maintenance and discarding of data based on classification. □ Identify the Data owners □ Access should be given based on data type confidentiality of the data |
| Storage of Information on desktops | <ul style="list-style-type: none"> □ No security control requirements | <ul style="list-style-type: none"> □ The desktop storing these documents must be protected by a password. Hard-copies | <ul style="list-style-type: none"> □ E-mails containing confidential information must be downloaded into to the local personal folder immediately on receiving the mail. This would prevent mails from being stored in the mail folders on mail servers and looked by system administrators. |

| Control Area | Public | Internal Use Only | Confidential |
|--------------|--------|--|---|
| | | <p>should be preferably kept under lock and key.</p> <ul style="list-style-type: none"> Hard disk should not be shared at the drive levels, and shared folders should be restricted to known individuals. | <ul style="list-style-type: none"> For backup purpose all confidential documents should be stored on the respective user's folder of the file server. They should preferably be password protected. Confidential documents should not be stored on the public directories of the file server. Complete Hard drive of desktop shall not be shared on the network. On need basis, selected folders on the hard drive can be shared, and access be given to named individuals. Data shall be encrypted additional controls may be required to be deployed depending on the sensitivity of data, other access controls might suffice. |

| Control Area | Public | Internal Use Only | Confidential |
|--|--|---|--|
| Storage of Information Medium (e.g. diskettes, CD, hard copy) | <ul style="list-style-type: none"> No security control requirements | <ul style="list-style-type: none"> Medium should preferably be stored in a personal storage shelf, preferably, locked. | <ul style="list-style-type: none"> The information should be kept in a separate cabinet preferably a fireproof cabinet. The authority to manage the cabinet will be done by a person nominated by the department head. Access to the information / cabinet shall be granted by the department head by E-mail. Any confidential information, which is to be kept or retrieved from the cabinet, will be done in front of the designated person. Any hard copy documents that cannot be reproduced (like legal contracts, third party contracts) should also be kept preferably in the fireproof cabinets. |

| Labeling of Information | <input type="checkbox"/> No Labeling | <input type="checkbox"/> The document/record (electronic form) must | <input type="checkbox"/> The document/record (electronic form) must contain the information |
|--|---|---|---|
| (documents and Records – soft copy) | Required | <p>contain the information classification logo with the classification identified as 'Internal Use Only' at the start of the document/record. The document/record(Hard copy) should have the information classification logo as a cover page or as part of the title page with the classification identified as "Internal Use Only"</p> <p><input type="checkbox"/> For email communication, the attached document should have the classification "Internal Use Only" marked on the first page.</p> | <p>classification logo with the classification identified as 'Confidential' at the start of the document/record. The document/record(Hard copy) should have the information classification logo as a cover page or as part of the title page with the classification identified as "Confidential"</p> <p><input type="checkbox"/> The information owner will do the labeling of the document and if any doubt is there while classifying the information then he / she should take concurrence from departmental head.</p> <p><input type="checkbox"/> All email communication of confidential information must have 'Confidential' as the first word in the subject</p> <p><input type="checkbox"/> Data shall be labelled as per information asset classification at the time of storage and transfer.</p> |
| Labeling of Information Medium (e.g. diskettes, CD, hard copy) | <input type="checkbox"/> No Labeling Required | <input type="checkbox"/> No Labeling Required | <input type="checkbox"/> The information medium must be marked ' Confidential ' |
| Control Area | Public | Internal Use Only | Confidential |

| | | | |
|----------------------------------|------------------------------------|------------------------------------|---|
| Addressing/ Packaging | ☐ No security control requirements | ☐ No security control requirements | <ul style="list-style-type: none"> ☐ The storage medium must have two envelopes/layers of packaging ☐ The outer envelope/layer must show the recipients name and address, be marked 'To be opened by addressee only', and show the name and phone number of the sender of the information |
| | | | <ul style="list-style-type: none"> ☐ The inner envelope / layer should be marked as “Confidential”. |

| | | | |
|--|--|---|--|
| Dispatch and Distribution of Information (except EMail) | <ul style="list-style-type: none"> □ No security control requirements | <ul style="list-style-type: none"> □ Packaging shall ensure physical protection of the item □ Normal mail service or by any courier □ This information can be freely circulated only to the internal Trianz employees □ Circulation of Internal Use Only document to any third party and/or to anyone outside Trianz shall require approval from the head of concerned department. The document shall be detailed about the data retention period based on regulatory, sensitivity and information classification as required. □ The validity of data classification needs to be checked on a periodic basis. If there is any change, data should be reclassified accordingly. | <ul style="list-style-type: none"> □ Packaging must ensure physical protection of the item □ Dispatch or distribution of information to anyone outside his/her department, third party and/or outsourced party should be by hand or approved courier □ Printed information sent through internal mail, external mail, or by courier must be sent by trusted courier or registered mail. The method of mailing must provide tracking. □ Distribution is to named individual(s) only □ Confidential information cannot be taken out of Trianz premises in form of media like Hard Copy, CD, Floppy, USB etc. without prior permission of department head. |
|--|--|---|--|

| Control Area | Public | Internal Use Only | Confidential |
|---|---|--|--|
| Dispatch and Distribution of Information (Electronic Mail) | <ul style="list-style-type: none"> No security control requirements | <ul style="list-style-type: none"> Possible to send email containing information to internal employees without any explicit approval from Trianz authority. Circulation of Internal document to any third party and/or to anyone outside Trianz shall require approval from the head of concerned department through Email and marking a copy to him / her while sending the document. | <ul style="list-style-type: none"> Circulation of confidential document to any third party and/or to anyone outside Trianz shall require approval from the head of concerned department through E-mail and marking a copy to him / her while sending the document. BCC while emailing is not permitted for “Confidential” documents. While sending the document to any authorized person it should be marked as “Confidential” in the subject or body of the mail in such a fashion that the mark is easily visible. Data shall be encrypted while in transfer using appropriate encryption methodologies. |
| Voice | <ul style="list-style-type: none"> No security control required | <ul style="list-style-type: none"> No security control required | <ul style="list-style-type: none"> It must not be discussed on speakerphones or during teleconferences unless all participating parties first acknowledge that no unauthorized persons are in close proximity, such that they might overhear the conversation |
| Disposal of Information | <ul style="list-style-type: none"> These documents may be used for draft (reverse side) printing | <ul style="list-style-type: none"> These documents should NOT be used for draft (reverse side) printing. These documents may be destroyed manually, ensuring that the document may not be reconstructed easily. | <ul style="list-style-type: none"> Any information should be destroyed / deleted, only after the minimum retention period, when the information is obsolete or no longer needed. Any hard copy confidential document, which is to be destroyed, should be destroyed by tearing into small pieces preferably using the shredder at that moment of time. Any confidential information present in CD where it cannot be deleted from the electronic media should be physically destroyed. |

| | | | |
|--|--|--|--|
| | | | <ul style="list-style-type: none"> □ Any hard disk containing confidential information should undergo low level formatting, so that information cannot be recovered from that hard disk. □ Secure disposal of data (including the disks etc.) shall be documented. |
|--|--|--|--|

2. References:

- IT Operation Process
- Information Asset classification Policy
- Access Control Policy
- ISMS TMR Template
- Acceptable Usage Policy
- ISMS Apex Manual
- Media Handling Policy
- Policy on the Use of Cryptographic Control
- Data Modelling Using UML Guidelines
- Asset Tracking Sheet Template

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

| Ver. No. | Author | Reviewer | Approver | Date | Reason for Change | Change Description |
|----------|-----------------|----------|----------|------------|---------------------------------------|--|
| 0.00 | Jyotessh G Nair | | | 19-Feb07 | Initial Draft | None |
| 1.00 | Jyotessh G Nair | | | 26-Feb-07 | Baseline is approved by Zulfikar Deen | Approved Baseline. |
| 1.01 | Bharateesha B R | | | 24-Feb-09 | New Asset Management Framework | Formatted the document to incorporate the new asset management framework |
| 1.02 | Bharateesha B R | | | 11- Mar-09 | New Asset Management Framework | Included Records in the scope of section Labeling Of Information – Soft Copy. Made changes to the Guidelines for each classification. |
| 2.00 | Balu Nair | | | 28-Apr-09 | Approved for Baseline | Baselined |
| 2.01 | Bharateesha B R | | | 23-June-09 | 2 nd Surveillance audit | Removed “Hard Copy” for the control area “ Labeling of Information (documents and Records – soft copy) Changed the point 3 of the guidelines for control area “Dispatch and Distribution of |

| | | | | | | |
|------|-----------------|--|--|------------|---|--|
| | | | | | | Information (Electronic Mail) for the classification “Confidential” |
| 3.00 | Bharateesha B R | | | 23-June-09 | Approval for Baseline | Baselined |
| 3.01 | Chakravarthi | | | 30-Dec-10 | QMG review | Formatted entire document |
| 4.00 | Chakravarthi | | | 31-Dec-10 | Request for approval | Baselined |
| 4.01 | Srilakshmi | | | 24-May-11 | QMG Review | Modified release id in header and cover page |
| 5.00 | Srilakshmi | | | 24-May-11 | Approval for Baseline | Baselined |
| 5.01 | Sudharsana | | | 3-Aug-11 | QMG review | Replace Owner with Management Representative in place of CIO Removed Retention period in Document Classification scheme section |
| 6.00 | Sudharsana | | | 3-Aug-11 | Request for Approval | Approved and Base lined |
| 7.00 | Balu Nair | | | 08-Nov-12 | Standardization of Blue Book Process Assets | Modified the template format Changed the Logo |

| | | | | | | |
|------|------------------------------|--|--|-----------|--|--|
| 7.01 | Paramita Ghosh and Balu Nair | | | 25-Jan-16 | Client Audit and alignment with shared assessment checklist. | <p>Handling of information based on the type of Information Asset Classification.</p> <p>Updated control areas to include below points</p> |
| | | | | | | <p>Added identification of data owners, criteria of accessing the data based on confidentiality, labelling mechanism for the sensitive documents, validation of data classification which needs to be verified on a periodic basis, data retention period based on regulatory, sensitivity and information, appropriate encryption methodologies for data in transit and documentation of securely disposal of data</p> <p>All the confidential/sensitive data shall be encrypted. data.</p> <p>Added separate "REFERENCES" sections</p> |
| 8.00 | Balu Nair | | | 08-Feb-16 | Approved by Mahesh (CISO) | Baselined |

| | | | | | | |
|------|-----------|--------|------------|-----------|-------------------|----------------------------|
| 8.1 | Karthik N | | | 3-Jan-22 | For Review | Migrated to new template |
| 9.0 | Karthik N | Siva N | Siva N | 3-Jan-22 | For Approval | Approved and Baselined |
| 9.0 | Kruti | Vijaya | | 3-June-24 | Annual Review | No Changes |
| 9.1 | Vijaya | Balu | | 26-May-25 | For Annual Review | Migrated to a new template |
| 10.0 | Vijaya | Balu | Srikanth M | 29-May-25 | For Approval | Approved and Baselined |



Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com



The content in this document is copyrighted; any unauthorized use – in part or full – may violate the copyright, trademark, and other laws. This document may not be modified, reproduced, or publicly displayed, performed, or distributed, or used for any public or commercial purposes. The Trianz name and its products are subject to trademark and copyright protections, regardless of how and where referenced.