INFORMATION SECURITY POLICY

A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED

V 1.0 - GDPR

TABLE OF CONTENTS

General Policy

In this policy, 'information security' is defined as:

Preserving

This means that management, all full time or part time Employees and Staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. All Employees and Staff will receive information security awareness training and more specialised Employees and Staff will receive appropriately specialised information security training.

the availability,

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

confidentiality

This involves ensuring that information, which falls within the scope of the Data Protection Regulation 679/2016/EU is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to such information when kept by A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED and its systems [including its network(s), website(s), extranet(s), and / or e-commerce systems].

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency including for network(s), e-commerce system(s), website(s), extranet(s) and data backup plans and security incident reporting. A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED must comply with all relevant data-related legislation in those jurisdictions within which it operates.

General Policy

---

of the physical (assets)

The physical assets of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

and information assets

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED.

A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED and such partners that are part of our integrated network and have signed up to our security policy and have accepted our ISMS.

The ISMS is the Information Security Management System, of which this policy and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO 27001:2013.

A **SECURITY BREACH** is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED.

Assignment of consequences

---

1. Responsibilities

The Data Protection Officer is responsible for ensuring that all necessary competences are identified for the personal information management system (PIMS). HR Department is responsible for ensuring that all job descriptions include the identified competencies, and for maintaining records of relevant qualifications, experience and training.

2. Procedure

Identifying competence:

The Data Protection Officer identifies necessary competence for all Employees and Staff working in roles with day-to-day responsibilities involving personal data and processing operations, and/or those with permanent and regular access to personal data. These competences are recorded in competence matrix.

When hiring new employees who will be in a role involved in personal data and processing, the job description includes the identified competencies in accordance with Data Protection Officer (DPO) Job Description as per Data Protection Manual and DPO's Job Description.

When developing a new role within the personal information management system, a job description is developed using the identified competencies, in accordance with the appendices to the Data Protection Manual.

Recognition of competence:

Persons doing work under the control of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED are required to have all essential competencies identified for that role in the competence matrix.

Evidence of competence identified as necessary is retained as part of the individual's HR Department records. A person can be deemed competent on the basis of qualification, experience or training.

Where specific data protection qualifications, experience or training are explicitly necessary, this is identified in the competence matrix by the Data Protection Officer.

Where qualifications are time-limited or require ongoing maintenance (such as continuing profession development), A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED maintains records that provide evidence of the individual's maintenance of their qualification.

Assignment of consequences

Acquiring competence:

A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD AND DENCHRI LIMITED acquires appropriate competence for its personal information management system through the following methods:

- Hiring suitably competent individuals
- Contracting third parties
- Training existing staff

A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's hiring and contracting is conducted in accordance with the procedures above (3.1 and 3.2) to identify and recognise appropriate competence.

A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's provision of training is conducted in accordance with the GDPR Training Policy as described in the Data Protection Manual and as per training schedules elaborated by the DPO.

Communication Procedure

Responsibilities

- Data Protection Officer (DPO) is responsible for identifying any necessary internal/external communications relating to compliance with the Data Protection Regulation 679/2016/EU.
- The Processing unit is responsible for identifying when internal or external communication will be necessary.

- The DPO is responsible for identifying requirements for internal and external communications and scheduling any necessary regular internal communications relevant to the Data Protection Regulation 679/2016/EU.
- All Heads of Departments are responsible for determining requirements for external communications and approving external communications and report deficiencies to their reporting line.

Internal communications

The DPO identifies the necessity for internal communication based on how a complaint by a data subject is resolved and / or if the internal communication channels proof to be inefficient.

The Data Protection Officer identifies the content of the communication according to the following conditions:

- Cause for the communication
- Classification of the information being communicated
- Classification of the communication itself
- Other, subject to the circumstances on a case-by-case base

The Data Protection Officer identifies the appropriate audience for the communication according to the following conditions:

- Nature of the information being communicated
- Reporting lines and Duties per department
- The medium of communication (e.g. email, staff room notice, mandatory signed notification, etc.)
- Other, in relation to the specific case

The Data Protection Officer composes the communication as appropriate. The communication is subject to review and approval by a Department of the corporate structure of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED.

Communication Procedure

External communications

A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED is part of the following information sharing networks:

Third party agreements as per corporate organizational structure, as per Internal Operations Manual, as per Data Protection Manual.

The Data Protection Officer identifies the necessity for external communication based on contractual or statutory obligations, business need, an organisational transparency policy, etc.

The Data Protection Officer makes available the contact details of the Data Protection Officer as well as to data subjects and the Data Protection Commission.

The Data Protection Officer identifies the content of the communication according to the following conditions:

- Cause for the communication
- Classification of the information being communicated
- Classification of related information
- Other

The Data Protection Officer identifies the appropriate audience for the communication according to the following conditions:

- Cause for the communication
- Classification of the information being communicated
- Contractual, statutory or regulatory obligations
- The medium of communication (e.g. email, staff room notice, mandatory signed notification, etc.)
- Other

The Data Protection Officer composes the communication as appropriate, in accordance with A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's style guide for external communications.

The communication is subject to review and approval by departments according to the corporate structure of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED.

Document Control

Responsibilities

The person inside the corporate and / or organizational structure of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD /

THEOSERVICES LTD and DENCHRI LIMITED, who follows and works on any document related to the Data Protection standards, is responsible for this procedure.

Procedure
Documents are appropriately identified and described. Within the document, the following information is provided:

- Title
- Date of last revision
- Owner
- Document reference
- Classification
- Other

The document is externally labelled (e.g. filename, metadata, sticker) with the following information:

- Title
- Document reference
- Other

Ensuring that all changes to the document are identified, both by means of Word's *track changes* function and in a *Change History Record* at the end of the document, and that the current issue no and issue date are correct.

Documentation is kept in an appropriate format and media. Approving the document for adequacy prior to its submission for formal release, authorisation to the appropriate level of management.

Ensuring that distribution of such a document is controlled, in line with the instructions in Clause 4 of this procedure.

Document Control

Ensuring that all such documents are subject to appropriate classification levels, in line with the requirements of ISO 27002:2013 the Data Protection Regulation 679/2016/EU.

Ensuring, by means of periodic reviews, that all such documents within the Data Protection Regulation 679/2016/EU are up to date and, where they are not, ensuring that (subject to Clause 5 below) they are updated, re-approved and re-issued.

The policies, procedures and work instructions are all published centrally on the Intranet Server of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/

THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED. This central set of Data Protection documentation is available to all users of information and personal data assets of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED and all pages of all documents contain hidden text, revealed on printing, which indicates that the printed version of the document is 'uncontrolled' – i.e. it is not a current, authorised excerpt from the Data Protection documentation.

Ensuring that the most recent version of the documents is available at the identified points of use (an authorised list of these points is attached to this procedure).

Ensuring that the document remains legible and readily identifiable as being part of the corporate governance at A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED, which concerns Data Protection standards.

Ensuring that documents that originate outside of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC/ THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED, but which need to be protected or controlled as part of the Data Protection standard are incorporated into A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's document classification, version control and management requirements by means of internal review and approval for adoption.

Ensuring that obsolete documents are withdrawn from when updated versions are issued.

If there is a reason for retaining them, ensuring that they are clearly marked 'obsolete – not to be used after [date]'.

Document Control

Document Control

Documents required by the Data Protection Regulation 679/2016/EU must be controlled. Records have additional security requirements and must be controlled according to the requirements of this procedure.

Header

Document title: the subject it addresses and the tier it forms part of; is it a policy (tier 1), procedure (tier 2), work instruction or plan (tier 3), record (tier 4).

Document reference: This is a reference number that ties the document firmly into the overall structure of the corporate governance related to the requirements of the Data Protection Regulation 679/2016/EU. All these documents that are not records have a fixed 'DOC' prefix, records use a fixed 'REC' prefix. Documents have the prefix GDPR and then a sequential numeric identifier.

Issue number: the first time a document goes out, it will be Issue 1; a revised version will be Issue 2, etc.

Issue date: the date on which this issue (with this issue number) was authorised and issued.

Page: the current page number and the number of pages that this issue has (automated entries through the *Header and Footer* toolbar) – so that the reader can be clear that none have been missed.

Final Paragraph

The owner of the document, who issued and is responsible for keeping it up to date, needs to be identified – by role, not by name.

The places where a current version of the document can be viewed by those it is intended for should be clearly stated and this must tie in to the list identified in Clause 3.9 above.

Approval: the master copy of this document needs to be physically signed and dated by whoever is authorised to approve and issue it. The master copy is retained within the master record set.

Change History Record: there needs to be a section, at the bottom of the master copy, which describes the history of changes, showing the dates of issue for each of the earlier versions and which summarises both the changes and reasons for them in each of the earlier versions.

Document Control

Footer

- The security classification needs to be shown, if this is relevant.
- The version number of the document is recorded here.

Change Management

Changes to the policies and procedures (including updating, withdrawal or replacement) must be authorised in line with the requirements of Data Protection Regulation 679/2016/EU.

All changes are subject to, and a consequence of, a change in the risk assessment. A summary of the changed risk assessment must, therefore, be attached to the file version of the original document prior to authorisation of the changes.

Monitoring

Responsibilities

The Data Protection Officer is responsible for determining the requirements for monitoring, measurement, analysis and evaluation of data protection and compliance with the Data Protection Regulation 679/2016/EU.

Each person at A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED processing data is responsible for ensuring that processes under their control are appropriately monitored and measured.

The Data Protection Officer is responsible for the conduct of analysis and evaluation of monitoring and measurement results.

Procedure (ISO27001: 2013)

The Data Protection Officer identifies processes that require monitoring and measurement, according to the following conditions:

- The process produces results or by-products that can be quantitatively measured
- The process affects the following processes
- The process is the result of other processes
- The process generates error reports or other evidence of non-conformance.

The Data Protection Officer ensures that A. CHR. THEOPHILOU LLC / A. THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD AND DENCHRI LIMITED's monitoring and measurement activities are listed in Data Protection manual.

The DPO monitors the process and collates measurements on a regular base, but at least monthly by:

Automated process; or
Manual process

The measurements are submitted to the Data Protection Officer every three months. The Data Protection Officer identifies appropriately qualified persons to analyse and evaluate the results of the monitoring and measurement, which is conducted monthly.

Monitoring

Results of monitoring and measurement are analysed by the mechanism of stress testing as for the Risk Management manual and by the revision of physically and electronically stored documents per each department.

Results of monitoring, measurement and analysis are evaluated against the requirements of the relevant PIMS and Data Protection regulation 679/2016/EU.

Results of the analysis and evaluation are documented in the report by the DPO and submitted to the management for review.

Data Protection Policy Management Review Procedure

Responsibilities

- The Data Protection Officer, who is the defined owner of the Data Protection Policy, is responsible for its development, review and evaluation.
- These documents include [Include details of the owners of other information security and personal data policies you may have developed.]
- Board of Directors is responsible for carrying out reviews in line with this procedure and for driving compliance to the Data Protection Regulation 679/2016/EU.
- The Head of IT (CIO) is responsible for convening meetings of the Board of Directors, either after there have been (or it is planned that there will be) significant changes in the organizational environment, business circumstances, legal conditions or technical environment, and which is likely to have an impact on the level of risk facing personal data, or at least annually.

Monitoring

Management review inputs

Management reviews must consider:

- Status of actions from previous management reviews
- Changes in internal and external issues relevant to the Data Protection Regulation 679/2016/EU
- Information on GDPR performance including trends in

    - Nonconformities and corrective actions
    - Monitoring and measurement evaluation results
    - Internal and external audit reports
    - Results and/or trends from the measurement of progress towards the protection of information security and personal data.

Performance for compliance with the Data Protection Regulation 679/2016/EU must be considered, including

- Follow-up actions from previous management reviews
- Need for changes including its policy and objectives
- Opportunities for improvement
- Results of audits and reviews
- Xsd Results of audits and reviews of key suppliers and partners
- Techniques, products or services which could be used to improve compliance with the Data Protection Regulation 679/2016/EU.
- Status of corrective actions
- Results of exercises and tests
- Risks or issues not adequately addressed
- Changes (internal or external) that could affect compliance with the Data Protection Regulation 679/2016/EU
- Adequacy of Data Protection Policy
- Recommendations for improvement (internally or externally generated)
- Lessons learned
- Actions arising from disruptive incidents (post-incident reports)
- Emerging good practice and guidance

Monitoring

Management review outputs

Improving A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's assessment of the risks, including updating the risk assessment and incident management plans.

Any variations to the scope of the Data Protection Regulation 679/2016/EU that may be required.

Modifying or improving the policies and procedures and their effectiveness, ensuring that any changes to business or business processes, or changes to statutory, regulatory or contractual requirements are accommodated.

Update of risk assessments, plans and related procedures.

Modification of procedures and controls to respond to internal or external events that may impact compliance with the Data Protection Regulation 679/2016/EU, including changes to:

- Business and operational requirements
- Risk reduction and security requirements
- Operational conditions and processes
- Legal and regulatory requirements
- Contractual obligations
- Levels of risk; criteria for accepting risks
- Resource needs
- Funding and budget requirements

Monitoring

Reviewing and improving how the effectiveness of controls is measured.

Improving the allocation of resources and responsibilities, including ensuring that complying with the Data Protection Regulation 679/2016/EU is supported by adequate resources, funding and budget.

Formulating and agreeing any changes to the Data Protection Policy which would be necessary to give effect to any improvements identified.

The Data Protection Officer is responsible for ensuring that the review meeting is recorded and consistent with the requirements of the Data Protection Regulation 679/2016/EU to retain records of reviews, and to review and update processing operations where necessary. The record is signed by its chair, and required actions identified for follow up.

The Data Protection Officer is responsible for ensuring that:

- results of management reviews are communicated as appropriate to relevant interested parties;
- appropriate actions are taken as a result of management review.

Board of Directors must approve any changes to the policy at its next scheduled meeting and prior to its implementation.

Nonconformity and Corrective Action Procedure

Responsibilities for this procedure

Every individual involved directly or indirectly with A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC/ THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED is responsible for initiating and complying with this procedure as and whenever it applies, and involves them.

The Data Protection Officer is responsible for the overall control and operation of this procedure and for coordinating and processing all Non-Conformance Reports.

Each Department Manager as per reporting line is responsible for progressing Non-Conformance Reports that are capable of resolution within their area, and forwarding them, and others, to the Quality Manager (i.e. the DPO).

Procedure [ISO27001]

- When a problem or potential improvement is identified, each of the Employees or Staff of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED has a duty to inform their Head of department as per reporting line of the issue, either verbally or by using a Non-Conformance Report (Annex).
- Any Employees or Staff or third party who becomes aware of an issue which does not meet A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's defined approach and standards, or which has the potential for such an adverse effect, must raise a Non-Conformance Report immediately and forward it to the appropriate Head of Department or Manager as per reporting line.
- The DPO maintains a Non-Conformance Report Log (Annex). For actions within their area of responsibility, each Head of Department will evaluate whether the issue is valid and its priority.
- The Head of Department determines whether the nonconformity is isolated, if there are similar nonconformities, or if the cause of the nonconformity has resulted or could result in other nonconformities.
- The Head of Department agrees a course of action and timescale to correct the issue, dependent upon the effect the issue is likely to have and to what degree.
- The agreed actions may rectify and prevent recurrence of the issue, or the consequences can be accepted. Such actions are recorded on the Non-Conformance Report and a copy is sent to the DPO.
- Actions to correct nonconformities will be reviewed as described below. As such, the Head of Department and the DPO will also need to agree a timeline for review and any necessary metrics for establishing whether the corrective action has been successful. These details are recorded on the Non-Conformance Report and mirrored in the copy held by the DPO.

- If related nonconformities as identified in here above remain untreated by the action determined in here above, the Head of Department will raise a new non-conformance report as detailed in here above and follow this procedure accordingly.

Nonconformity and Corrective Action Procedure

Timescales for completion should have regard to the cost/benefit of the non-conformance and other reasonable business priorities.

On receipt of forms with no log number, the Quality Manager assigns one, evaluates the report and forwards it to the appropriate Manager/Executive (generic/line) who will act as inhere above.

The DPO will regularly monitor the progress of outstanding Non-Conformance Reports. If any action has not been completed by the previously agreed date, she/he will agree and record new actions and/or dates. If not satisfied that achievable progress is being made, they will escalate the matter to higher line management responsible for that area.

Non-Conformity Reports will be closed down by the DPO once the issue has been addressed and proof of consideration to preventive measures can be demonstrated; this may result in a review by scheduled or additional Internal Audits. This is recorded on the Non-Conformance Report and the corresponding log entry is updated.

A copy of the completed form is sent to the originator (internally raised issues) for their information, (except in the cases of those generated at Internal Audit).

The DPO will review the effectiveness of any corrective action taken after a time period determined on the basis of the action and the nonconformity it addresses, as described in here, above. If the corrective action fails to adequately address the nonconformity, a new Non-Conformance Report should be raised to address it.

Continual improvement

Responsibilities

Every individual involved directly or indirectly with A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED is responsible for initiating and complying with this procedure as and when it applies, and involves them.

The Management System Owner (MSO) is responsible for the overall control and operation of this procedure and for progressing and co-ordinating all Non-Conformance Reports.

Each Head of Department is responsible for progressing Non-Conformance Reports that are capable of resolution within their area, and forwarding them and others to the Management System Owner (MSO).

Procedure

Sources of information that can drive continual improvement include

- Post-incident reports
- Exercise reports
- Audit and nonconformity reports
- Suggestions from staff, managers, and interested parties such as customers, partners, suppliers, local community, emergency services, regulators

Such information should be sent to the Management System Owner (MSO), either by delivering the report in question, verbally or by using a Non-Conformance Report Log (Annex).

If a corrective action (for a known problem) is required, the Management System Owner (MSO) should initiate a formal Corrective Action.

If a new risk or potential problem is identified, the DPO should feed it into the risk assessment process as appropriate, to trigger evaluation and possibly changing the PIMS to accommodate it.

Wireless Notebook Access

Responsibilities

The Head of IT (CIO) is responsible for specifying and/or providing the firewalls, anti-malware software, automatic updating, connectivity and backup facilities required under this procedure. The Head of HR is responsible for user training. All users have specific responsibilities in terms of their User Agreements.

Procedure [ISO 27002]

- A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED requires notebook computer level deployment of the company's specified firewalls, anti-malware software, and automatic updating facilities that are all up to date and meet the corporate minimum standards, which are specified in the Data Protection Manual and the Internal Operations Manual, as well as in the User Agreement.
- A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED

requires notebook computer level deployment of the corporate policy on usernames and passwords, to have a password protected screensaver, and to password protect and encrypt all folders containing confidential corporate information, and to disable folder and printer sharing, all of which is specified in the User Agreement.

- A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED requires notebook computers that carry personal data, or are able to connect to systems that store or process personal data, use full-disk encryption.
- A. CHR. THEOPHILOU LLC / AANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED requires that notebook computers are physically protected against theft and damage while in transit, in storage or in use and that, in cases of loss or theft, the specified corporate policy (see User Agreement) for dealing with such incidents is followed.
- A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED requires users (in the User Agreement) to ensure that all the most recent operating system and application security-related patches, fixes and updates have been installed.
- A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED requires (in the User Agreement) that notebook computers are backed up in line with corporate specifications.
- A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED requires users of notebook computers to carry with them at all times the chargers and spare batteries specified in the User Agreement.
- A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED requires users to comply with the corporate requirements on the means of connecting to public access points, and accessing corporate information, both as described in the User Agreement.
- A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED requires users, in the User Agreement, to act with care in public places so as to avoid the risk of screens and confidential notebook computer activity being overlooked by unauthorised persons.
- A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED carries out regular and ad hoc audits of all notebook computers to ensure that they are configured in compliance with this procedure.

Wireless Notebook Access

A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED provides users with

appropriate training and awareness to ensure that they understand the risks of wireless on the road computing and that they understand and can carry out their agreed security obligations. Work instruction sets out how the corporate requirements set out in here above are enforced.

Please refer to the Internal Security systems installed and maintained by the IT department for further reference and further information. It is the DPO's responsibility to ensure that these systems are adequate and sufficient as to prevent the unauthorized access of data, the loss or leakage of data being covered by the provisions of the Data Protection Regulation 679/2016/EU.

Wireless Notebook Access

---

1. A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED controls access to information on the basis of business and security requirements.
2. Access control rules and rights to applications, expressed in standard user profiles, for each user / group of users are clearly stated, together with the business requirements met by the controls.
3. The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.
4. The access rights to each application take into account:

    a. Premises access control – unauthorised persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems are located.
    b. System access control – access to data processing systems is prevented from being used without authorisation.
    c. Data access control – Persons entitled to use a data processing system gain access only to the data to which they have a right of access.
    d. Personal data cannot be read, copied, modified or removed without authorisation.
    e. The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the systems and network(s).
    f. Data protection (679/2016/EU) and privacy, legislation and contractual commitments regarding access to data or services.
    g. The 'need to know' principle (i.e. access is granted at the minimum level necessary for the role).
    h. 'Everything is generally forbidden unless expressly permitted'.
    i. Rules that must always be enforced and those that are only to be worked out by the DPO.
    j. Prohibit by access keys user initiated changes to information classification labels as in this policy.
    k. Prohibit user initiated changes to user permissions.
    l. Enforcing rules that require specific permission before enactment.
    m. Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

- A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED has standard user access profiles for common roles in A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED.
- Management of access rights across the network(s).
- User access requests, authorisation and administration are segregated as described in the Annex.
- User access requests are subject to formal authorisation, to periodic review and to removal.

Appendix

Internal Audit Lead Sheet

<table>
<tr><td colspan="2">Scope & Type of Audit: (incl. Site)

Technical Compliance / Compliance *</td><td>Report No.

Date

Auditors:</td></tr>
<tr><td>Persons Contacted:

Head of Internal Audit:</td><td></td><td>Previous Audit

Ref. No.

Principal Auditee’s

Signature</td></tr>
<tr><td>Management System
Documentation/Aspects Covered:</td><td></td><td></td></tr>
<tr><td>Summary of Audit:</td><td>No. of Non-conformities:</td><td>No. of Observations:</td></tr>
</table>

Head of Internal Audit's Signature:	Date:

Incident/Improvement Action Reports Raised: (Ticked box = completed)

1.	☐	2.	☐	3.	☐
4.	☐	5.	☐	6.	☐
7.	☐	8.	☐	9.	☐
10.	☐	11.	☐	12.	☐

Quality Manager's Signature	Date:
(Actions Completed):	

Management Review Record

Topic	Outcome	Action?	Responsible	Target Date
Results of audits				
Feedback (Customers, internal, etc.)				
Process performance and product, service, process or control conformity				
Status of corrective action(s)				
Follow-up actions from previous management reviews				
Changes that could affect the integrated management system				
Recommendations for improvement				
Improvement of the effectiveness of the integrated management system and its processes				
Improvement of product, service, process or control related to stakeholder requirement				
Resource needs				
Techniques, products or services that may improve GDPR compliance				

Corrective Action Report

	Corrective Action Report	**No. Assigned by [xxx Mgr.]**
	Issue, or potential issue, identified (describe the problem as fully as possible):	
	By: Date:	
	Now pass to [xxx Manager]	

	Assignee: Please complete and return this report within 10 working days of receipt	
Assignee	Root cause (Why did it happen or why might it happen?):	
	Immediate Corrective Action (What will be done now? If no corrective action is to be made, justify the reasons for this.):	

	Preventive Action (What will be done to ever stop the problem happening or happening again? What changes will be made to the management system?):
	To be completed by: [date] By:
[xxx Mgr] / Originator	Outcome (What happened?):
	Closed By: Date of closing:

Nonconformance Report

Originator: (Person completing report)	**Date Raised:**	Log Ref. Number	
Details of Non-Conformity:			
Review by auditee: (Miscellaneous comments and initials to demonstrate review) **Initials:** Send to Quality Manager as part of Audit Rep			
Views: (For completion by responsible Management Team member only) Send to Quality Manager			
Suggested Actions:	Action by:	Target Date:	Date Finished (& initial)

Conclusion: (For completion by Quality Manager)

Signed: **Date:**

Originator told of result:	**Recurrence Monitored by:**	**Date:**	**Audit Ref:**

Information Security Report

Name of person making report:

Position/role/status:

Name and title of line manager:

[Office/location]

Date and time of report:

This report concerns:

System/information asset description:

[Identifying serial number/asset number/system name/other mark]

Weakness or event:

Date and time weakness or event observed:

Observed by whom (if not person making the report):

Description of weakness or event:

[Please provide as much detailed information as possible: what malfunctioned, what (sequence of) actions you were executing at the time, what messages came up on your screen, what precise things or strange behaviour occurred, what appeared to be the breach or other issue, what services, facilities or equipment ceased to be available, awareness of any human errors or non-compliance with organisational policies, procedures or work instructions, or breaches of physical security.]

EVENT ASSESSMENT

Initial analysis:

Event Incident Vulnerability Unknown

Reasons for assessment:

Final analysis

Signed:

(Person making this report)

The box below is for use by the Data Protection Officer

Individual User Agreement

1. Name: [1]

Position:

Department:

Access rights and levels of confidentiality the user is entitled to access:

User access request originated by:

[Date]

User access request approved by: Manager/Executive (generic/line)

[Date]

User access request approved by: *[Asset owner(s)]*

[Date]

User acceptance of access rights and responsibilities as set out in this agreement:

Signed and agreed by staff member:

[Date]

User access name allocated:

E-mail address allocated:

Data storage file allocated:

User access request processed: IT Department

[Date]

1.1 I, *[ ],* accept that I have been granted the access rights defined in this agreement to those organisational information assets also identified in this agreement. I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorised to access – including any

attempts to read, copy, modify or remove any personal data without prior authorisation - may lead to disciplinary action and specific sanctions. I also accept and will abide by A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's *[Internet Acceptable Use Policy, its e-mail policy and its information security weakness and event reporting policy]*. I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's disciplinary policy.

1.2 I acknowledge that I have received adequate training in all aspects of my use of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's systems and of my responsibilities under this agreement.

2. Passwords

2.1 My username and password will be issued in line with A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's procedure for authorizing and issuing them.

2.2 I will change my initial temporary password at first logon.

2.3 I will select and use passwords that are at least 7 characters in length, are alpha-numeric, are not based on any easily guessable or memorable data such as names, dates of birth, telephone numbers etc., are not dictionary words and are free of consecutive identical all-numeric or all-alphabetic characters.

2.4 I will keep my password secret and will not under any conditions divulge it to or share it with anyone, nor will I write it down and leave it anywhere that it can easily be found by someone else or record it anywhere without having obtained the specific authorisation of the DPO to do so.

2.5 I will not store my password in any automated logon process.

2.6 I will change my password at intervals as required by Organisation Name, will not attempt to re-use passwords or use new passwords that are in a sequence, and will change my password more frequently if there is evidence of possible system or password compromise.

2.7 I will not use the same password for organisational and personal use.

2.8 Replacement passwords are administered as set out inhere; users must obtain the written permission of their Manager/Executive (generic/line) before a replacement password can be issued.

2.9 *[Insert any additional information regarding additional authentication requirements, e.g. biometrics, tokens, etc.]*

3. Clear desk policy, screen savers and information reproduction

3.1 I understand that I am required to ensure that no confidential or restricted information (in paper or removable storage media format) is left on my desk, in my environs, or left in or near reproduction equipment (photocopiers, fax machines, scanners) when I am not in attendance and will ensure that such information is secured in line with A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's security requirements as set out inhere.

3.2 I understand that I am required to ensure that no one is able to access my workstation when I am not in attendance and that I must have a password protected screensaver that operates within *[five]* minutes of no activity or which I activate when I leave the workstation unattended.

3.3 I know that I am required to terminate active computer sessions when I have finished them and to log off (i.e. not simply turn off the computer screen) whenever I am finished working *[and that the workstation is to be protected by appropriate key locks when I am away from the building]*.

3.4 I accept that I am not allowed to *[use/bring in to the office]* personal storage media, MP3 players, digital cameras and mobile phones with photographic capability.

3.5 I accept that I may only use A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's reproductive equipment (photocopiers, fax machines, scanners) for proper organisational purposes and that I will ensure that I will use facilities that are appropriate for the classification level of any information with which I am dealing.

4. Software

4.1 I will ensure that no attempts are made to disable or over-ride any of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's installed software, including anti-malware software, firewalls and automatic updating services.

4.2 I accept that I may not download from the Internet or install on any organisational computer or other device any software of any sort for which A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED does not have a valid licence and that has not had the prior authorisation of the Head of IT (CIO). I recognise that this prohibition includes freeware, shareware, screensavers, toolbars and/or any other programs that might be available.

4.3 I recognise that A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's requirements in respect of the use of Instant Messenger facilities is *[ ]* and will abide by it.

5. Data control and legislation

5.1 I will obtain the written authorisation of the Data Protection Officer / GDPR Owner for the storage of any personal data (mine or anyone else's) on A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED's computer systems.

5.2 I will ensure that I abide by any legal requirements in respect of my computer use, including privacy and data protection regulations.

6. Backup and information classification

6.1 I acknowledge that I am responsible for ensuring that all information on my *[workstation]* is correctly classified and labelled in line with the requirements of the Data Protection Regulation 679/2016/EU. I will ensure that this requirement is complied with.

6.2 I acknowledge that I am responsible for backing up information on my *[workstation]*.

6.3 I understand that I am required to store all data *[where, how?]* and that I may not store information on the C:Drive of my computer.

7. Maintenance

7.1 I accept that I am responsible for the physical security of my workstation and will report any faults *[how?]* immediately.

8. Audit and security monitoring

[Set out here how you will handle monitoring, and what audits you will need to do.]

9. Revocation and change of access rights

[Set out here how you want to handle these issues.]

1. Classification of users

1.1 Users are also classified in terms of the level of access they need to information and systems. These classification levels, which are to be recorded in user agreements, are set out below:

Classification of data users		
Classification	**Access rights**	**Example**
Guest	Able to see and read public data. Full create and edit rights to a Private data space.	Clients
Trustee	Full rights to a shared directory or sub system. Able to see and use basic business templates and core information sources and systems.	Partner organisations Software maintenance Data input staff Anyone who has signed a non-disclosure agreement
Individual	Premises access – persons are permitted to gain physical access to premises, buildings or rooms where data processing systems are located. System access – access to data processing systems is permitted with prior authorisation. Data access – persons are entitled to use data processing systems in order to gain access to the data to which they have a right of access for their work only. Personal data cannot be read, copied, modified or removed without prior authorisation. Able to create files in a user group and delete owned files in that user group. Able to grant access rights to 'Private' files or directories to others. Access rights to restricted and confidential information dependent on role requirements.	
Supervisor	Full unrestricted rights to create new users and configure PCs and create user groups and manage the network.	IT staff

Classification of data users		
Classification	**Access rights**	**Example**
Administrator	Full unrestricted rights to defined systems and the ability to create and remove system supervisors.	IT Department [CEO] has right to read and edit all confidential/restricted documents

2. Privileges

2.1 Privileges are allocated in line with the requirements of the Information Security Policy of A. CHR. THEOPHILOU LLC / ANDREAS THEOPHILOU LLC / THEOSERVICES SECRETARIAL LIMITED/ THEOSERVICES NOMINEES LTD / THEOSERVICES LTD and DENCHRI LIMITED.
The available privileges for each operating system, application and other system in Organisation Name are: *[insert/attach a matrix or schedule that shows these, together with the level of user to which they could be allocated].*

3. User authentication

3.1 Users are authenticated at logon by providing both their username and their password within the parameters of the log-on system.
[This is where you should detail the other logon requirements that sit outside your single sign-on set up, and which might also refer to device authentication].