GDPR INFORMATION SECURITY POLICY

Date Created
17/04/2018

Status
Final

Version
1.0

Review Date
17/04/2019

1. POLICY STATEMENT

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.

The Board of Directors and management of EasTec UK Ltd, located at 16 Hackford Road, Hardingham, Norfolk, NR9 4ED, which operates in the educational sector are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout EasTec UK Ltd in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image.

EasTec UK Ltd current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks. In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy.

EasTec UK Ltd aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

All Employees/Staff of EasTec UK Ltd and certain external parties are expected to comply with this policy. The consequences of breaching the information security policy are set out in the disciplinary policy and in contracts and agreements with third parties.

Our systems are subject to continuous, systematic review and improvement. EasTec UK Ltd is committed to adhering to the principles of ISO27001:2013 and compliance with the GDPR.

2. INFORMATION SECURITY DEFINED

Preserving - This means that management, all full time or part time Employees/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.

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 EasTec UK Ltd 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 is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to

EasTec UK Ltd information and proprietary knowledge and its systems [including its network(s), website(s), extranet(s), and e-commerce systems].

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. EasTec UK Ltd must comply with all relevant data-related legislation in those jurisdictions within which it operates.

Physical (assets) - The physical assets of EasTec UK Ltd including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

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).

Security Breach - 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 EasTec UK Ltd.

3. TYPES OF INFORMATION SECURITY EVENTS

- Loss of service, functionality, equipment or other facilities
- System, software or hardware malfunctions, unscheduled shut downs, unexpected system errors or overloads
- Human errors
- Non-compliances with requirements of the ISMS (including uncontrolled system changes)
- Breaches of physical security arrangements
- Access violations

Note: this is not a conclusive list of information security events.

4. INFORMATION SECURITY CLASSIFICATION GUIDELINES

All EasTec UK Ltd information assets and services, and personal data activities are classified, taking into account their legality, value, sensitivity and criticality to EasTec UK Ltd.

The owner of each asset is responsible for its classification, for ensuring it is correctly labelled and for its correct handling in line with its classification. The intended recipient of any information assets sent from outside EasTec UK Ltd becomes the owner of that asset.

The Finance Director is responsible for maintaining the inventory of assets and services together with their classification levels. The Head of IT is responsible for the technical labelling mechanisms and is responsible for the creation, maintenance and review of electronic distribution lists and for ensuring that they conform to this security classification system.

All users of organisational information assets (including mobile phones, PDAs and other peripherals) have specific responsibilities identified in their user agreements.

Managers are responsible for ensuring that mail/postal services, voicemail and voice, fax, photocopiers, couriers, etc. services and sensitive documents (including cheques, invoices, headed notepaper) are handled in line with the requirements of the GDPR.

GDPR INFORMATION SECURITY POLICY

Date Created
17/04/2018

Status
Final

Version
1.0

Review Date
17/04/2019

Classification

EasTec UK Ltd classifies information into four levels of classification: confidential, restricted, private and public. The classification level of all assets is identified, both on the asset and in the information asset inventory.

The classification information must be included in the document footer, which must be manually set to appear on all pages of the document, or on the media on which it is recorded.

Information received from outside EasTec UK Ltd is reclassified by its recipient (who becomes its owner) so that, within EasTec UK Ltd, it complies with its procedure.

Information that is not marked with a classification level is returned to its sender for classification; if it cannot be returned, it is destroyed.

The classifications of information assets are regularly reviewed by their owner and if the classification level can be reduced, it will be. The asset owner is responsible for declassifying information.

Confidential: this classification applies to information that is specifically restricted to the Board of Directors and specific professional advisers. Information that falls into this category must be marked 'Confidential', and its circulation is kept to a minimum with the names of the people to whom it is limited identified on the document. Each copy of a document that has this level of classification is numbered and a register is retained identifying the recipient of each numbered copy.

Examples of confidential information might include information about potential acquisitions or corporate strategy, or about key organisational personnel, such as the Chief Executive Officer (CEO).

- Confidential information sent by email must be encrypted and digitally signed and sent only to the e-mail box of the identified recipient
- Confidential information can only be sent by fax if the nominated recipient is available to receive it directly from the fax machine.
- Confidential information can only be processed or stored on facilities that have been assessed as providing adequate security for such information. This classification is recorded on the information asset inventory and/or data inventory. The amount of information that falls into this category should be carefully limited.

Restricted: information of this category is restricted to Employees/Staff above a certain level. Examples of restricted information include draft statutory accounts, which might be available to everyone in senior management, or implementation plans for corporate restructuring, which senior managers need to work through prior to their being rolled out.

- Restricted information sent by email must be encrypted and digitally signed and sent only to the e-mail box of individuals known to be allowed to receive such information.
- Restricted information can only be sent by fax if a recipient from the required level is available to receive it directly from the fax machine.
- Restricted information can only be processed or stored on facilities which have been assessed as providing adequate security for such information. This classification is recorded on the information asset inventory and/or data inventory.

Private: this classification covers all information assets that have value, but which do not need to fall within either of the other categories. Everyone employed by EasTec UK Ltd is entitled to access information with this classification. This information has no restrictions in terms of how it is communicated, other than that it is not cleared for release outside EasTec UK Ltd.

Public: this is information which can be released outside EasTec UK Ltd.

Labelling

- Documents are labelled as set out above, in the document footer.
- Removable and storage media (CD-ROMs, USB sticks, tapes, etc.) are labelled
- Electronic documents and information assets are labelled
- Information processing facilities are labelled

Handling

Information assets can only be handled by individuals that have appropriate authorisations. The requirements for transmission, receipt, storage and declassification of classified and restricted information are described above. Destruction of information media can only be carried out by someone who has an appropriate level of authorisation.

EasTec UK Ltd requires that confidential documents are only circulated in secure pdf format / as read-only documents. Portable and storage media (including spooled media) must be moved, received and stored on the basis of the highest classification item recorded on them, and are subject to the physical security controls and are protected appropriately while being recorded.

For agreements with external organisations which include information sharing, include a matrix for translating their security classifications into this one.

5. RESPONDING TO INFORMATION SECURITY REPORTS

Users are required to report information security and personal data weaknesses, events or incidents to the Data Protection Office.

The information Security Manager is responsible for coordinating and managing the response to the any reported weakness, event or incident, including documentation of all emergency steps taken, evidence collection, and closing out the event. All technical staff and other Employees/Staff, contractors or third parties, are required to support The information Security Manager in dealing with an event, weakness or incident.

Procedure

The information Security Manager logs all information security and personal data reports immediately upon receipt, allocating to each a unique number and uses this log to ensure that all reports are analysed and closed out.

All information security and personal data events, weaknesses and incidents are, immediately upon receipt assessed and categorised by the data protection officer. Initially, there are four categories: events, vulnerabilities, incidents and unknowns.

Events are occurrences that, after analysis, have no or very minor importance for information security or personal data.

Vulnerabilities are weaknesses that, after analysis, clearly exist as significant weaknesses compromising information security or personal data.

Incidents are occurrences of events that have a significant probability of compromising EasTec UK Ltd information security or personal data.

Unknowns are those reported events or weaknesses that, after initial analysis, are still not capable of allocation to one of the four categories. The 'unknowns' are subject to further analysis to allocate them to one of the other three categories as soon as possible.

When there are multiple event reports in each category, the information Security Manager prioritises responses in the light of the criticality of the business systems and information assets (including personal data) at risk, the danger of further compromise to EasTec UK Ltd information security and personal data, the resources at his/her disposal, and any relevant time constraints (such as reporting requirements for personal data breaches).

Incidents involving high-value, business critical systems or personal data are immediately reported by the data protection officer.

The information Security Manager seeks additional input from qualified technical staff, as necessary and where he/she considers the standing instructions to be inadequate, to analyse and understand the incident and to identify appropriate actions to contain it and to implement contingency plans.

The information Security Manager invokes actions as set out in the standing work instructions plus additional activity that he/she considers necessary to contain and recover from the incident, and to implement contingency plans.

Where necessary, The information Security Manager coordinates activity with other organisations.

The information Security Manager confirms that the affected business systems have been restored and that the required controls are operational before authorising a return to normal working.

Once the incident is contained, and the required corrective action is completed, the Information Security Manager reports to CE with a summary of the incident, identifying the cause of the incident and analysing its progress, trying to identify how EasTec UK Ltd could have responded earlier or more effectively, or preventive action that might have been taken in advance of the information, the effectiveness of the containment and corrective actions and the contingency plans, and how the incident was closed out. The Information Security Manager is responsible for closing out the incident.

The Information Security Manager prepares a monthly report which identifies the number, type, category and severity of information security or personal data incidents during the preceding month, the cost of containment and recovery, and the total cost of the losses arising from each incident, and recommends (where appropriate) additional controls that might limit the frequency of information security and personal data incidents, improve EasTec UK Ltd ability to respond, and reduce the cost of response.

All the incident reports from the period since the last management review are taken into account at the next one, to ensure that EasTec UK Ltd learns from the incidents.

6. SECURE DISPOSAL OF STORAGE MEDIA

EasTec UK Ltd requires that all removable storage media are clean which means it is not possible to read or reconstitute the information that was stored on the device or document prior to disposal. All owners of removable storage media are responsible for ensuring that these media are disposed of in line with this procedure.

Procedure

- Hard disks must be cleared of all software and all organisational confidential and restricted information prior to disposal or reuse
- In the event that hard disks/media contain personal data, and it cannot be removed, then: Review whether or not you really do need to keep an archive within which this personal data is stored; it may well be that there is no overriding business reason for the archive in the first place.
- If you currently cannot technically delete archived data that is beyond its retention date, then to the hard disk/media needs to be put securely beyond use.

The Information Security Manager is responsible for the secure disposal of storage media and the disposal of all information processing equipment is routed through their office. A log is retained showing what media were destroyed and/or disposed of, and when. The information asset inventory and/or data inventory is adjusted once the asset has been disposed of.

- Hard disks are cleaned before disposal
- Devices containing confidential information are destroyed prior to disposal and are never reused.
- Devices containing confidential information that are damaged are subject to a risk assessment prior to sending for repair, to establish whether they should be repaired or replaced.
- Portable or removable storage media of any description are destroyed prior to disposal.
- All media are disposed of

Documents containing confidential and restricted information that are to be destroyed are shredded by their owners, using a shredder.

7. EXTERNAL PARTIES: INFORMATION SECURITY PROCEDURE

EasTec UK Ltd maintains the security of its information processing facilities and information assets in relation to external parties. All external parties who need to access any organisational information assets are subject to this procedure.

EasTec UK Ltd has (or may have) external party agreements with the following categories of organisations, all of whom are covered by this procedure; risks may be assessed for external parties as individual organisations or as categories, depending on the level of risk involved:

- Training providers
- Educational establishments
- Regulators, funding bodies

- Customers
- Outsourcing suppliers (facilities, operations, IT systems, data collection, call centers, others)
- Consultants and auditors
- Developers and suppliers of IT systems and services
- Temporary personnel, placement and other (casual) short-term appointments

The Data Protection Officer is responsible for services in any of the above categories that include personal data, is required to ensure that external parties have entered into a formal external party agreement under this procedure, and that transitions of information, information processing facilities, and any other information assets or personnel are planned and executed without a reduction in the level of security that existed prior to commencement of the transition.

The Data Protection Officer is responsible for ensuring that the security controls, service definitions and delivery levels included in external party agreements are implemented, maintained and operated by the external party.

Procedure
Where there is a business need for working with external parties, EasTec UK Ltd ensures that its information security is not reduced; access to organisational assets is not granted until a risk assessment has been completed, appropriate controls identified and implemented.

Risk Identification
EasTec UK Ltd carries out a risk assessment to identify risks related to external party access and the possible need to complete a data protection impact assessment.

The risk assessment identifies and documents, for each external party:

- The information processing facilities and information assets the external party will access.
- The type of access the third party will have – physical access and/or logical access (identifying the assets that will be accessed), whether the access is taking place on site or off site and the exact location from which access will be made.
- The value and classification of the information that will be accessed.
- The information assets that the external party are not intended to access, and which may require additional controls to secure.
- The external party's personnel, including their contractors and partners, who will or might be involved.
- How external party personnel are to be authenticated.
- How the external party will process, communicate and store information.
- The impact to the external party of access not being available when required, or of inaccurate or misleading information being entered, received or shared.
- How EasTec UK Ltd information security incident management procedure will be extended to incorporate information security incidents involving the external party.

- Any legal, regulatory or other contractual issues that should be taken into account with respect to the external party.
- How the interests of other stakeholders might be affected by any decisions.

EasTec UK Ltd implements those controls that are within its own power, and in line with the requirements of the GDPR.

EasTec UK Ltd agrees with the external party those controls that the external party is required to implement and documents them in an agreement that the third-party signs. The obligations on the external party include ensuring that all its personnel are aware of their obligations.

New controls, or changes to existing controls are identified, authorised, agreed with the third party, and made the subject of an agreed variation to the existing contract. The Data Protection Officer is responsible for ensuring that the revised controls are implemented and incorporated into the existing review and monitoring arrangements.