GDPR AUDIT PROCEDURE

TRENT VALLEY ELECTRICAL SERVICES LTD

Date Created	01/07/2018
Status	Final
Version	1.0
Review Date	01/07/2019
Owner	Data Protection Officer
Approved By	MD

1. SCOPE

This procedure applies to TRENT VALLEY ELECTRICAL SERVICES LTD internal audits, including any processing of high-risk personal data and any processing of personal data conducted by data processor subcontractors. It establishes the requirements for their planning, preparation, performance, reporting, following up and closing down.

The objective of this procedure is to establish an independent system for verification of personal information management systems (PIMS) and the GDPR, and its improvement by means of a controlled method for planning, scheduling, coordinating and performing internal audits, and related activities.

2. RESPONSIBILITIES

The Lead Auditor and Data Protection Officer are responsible for the overview and implementation of this procedure.

Appointed Internal Auditors are responsible for the preparation, execution and reporting of audits assigned to them for completion in accordance with their necessary competence and the requirements of this procedure. This may require third parties to be appointed to conduct internal audits to compensate where necessary expertise is not available.

All Employees/Staff are responsible for assisting in the audit process, as and when required.

3. PROCEDURE

The Lead Auditor shall establish an Audit Schedule of sufficient scope to ensure that each aspect of personal information management system and GDPR compliance is audited at least annually. It will identify the scope and frequency of audits, along with identifying the type of auditor (internal or supplier) to conduct the audit. The audit plan will be reviewed and agreed by the Chief Executive Officer (CEO).

The Lead Auditor will propose the audit plan at least 3 months in advance of the start date, programming audits with due consideration to:

- Business Need
- Severity of findings at most recent internal audit
- Programming of other audits in the same area
- Latest/proposed major revisions to processes, etc.
- Any other valid reason that may justly impact on the timing of an audit.

Audit performance will be reviewed as part of the management review. Audits will be assigned to an Internal Auditors who is competent to conduct that type of audit. Internal Auditors shall be deemed as ‘competent’ at the discretion of the Lead Auditor. Selection and conduct of audits will ensure objectivity and impartiality.

Internal Auditors may undergo a variety of development practices, to further develop their auditing skills, (e.g. accompanied audits and Internal Auditor meetings).

Date Created	01/07/2018
Status	Final
Version	1.0
Review Date	01/07/2019
Owner	Data Protection Officer
Approved By	MD

For specific types of audit, Internal Auditors will require special skills, (i.e. data protection and personal information for BS 10012:2017, technical audits for ISO 27001 compliance, ISO 22301 conformance, financial audits, etc.). Qualification requirements for the identified personnel are at the discretion of the Lead Auditor. Solution may be through the appointment of a suitable third party.

The Lead Auditor maintains a record of training received by Internal Auditors, and their suitability to conduct certain types of audit.

The Lead Auditor informs the Internal Auditors of the impending audit at least one month in advance of the required completion date. The Internal Auditors will be told the relevant audit number.

During the planning and preparation for an audit, the Internal Auditors ensure that the following actions are taken:

- Preparation of an audit checklist based upon audit.
- Contact the auditee to agree a mutually convenient date(s) for the audit and to discuss the scope of the audit.

The Internal Auditors conduct the audit using a checklist(s) as a guide. He/she examines the objective evidence and records relevant details.

The Data Protection Officer and Internal Auditors may expand a checklist if additional questions become necessary, to determine compliance with PIMS and GDPR, including any processing of high-risk personal data and any processing of personal data conducted by subcontracted data processors.

Confidentiality during audit: when an internal audit or third-party surveillance necessitates checking client files or databases, precautions must be taken to ensure that client confidentiality is preserved. Wherever possible, access is limited to satisfying the Internal Auditors that a file or database exists, is properly identified and is secure. If it is essential to check content, then access is limited to non-sensitive data.

During an audit, the Internal Auditors evaluate the evidence found and analyse the apparent non-conformances to ensure their validity as audit findings.

Where non-conformances are found, and the corrective action agreed, the Internal Auditors will note the actions against the non-conformance. Where actions were completed at time of audit the Internal Auditors may sign off the non-conformance.

Following completion of an audit, the Internal Auditors prepare a formal Audit Report.

Where the Internal Auditors use support documentation, this may be inserted into the Audit Report as observations, at the discretion of the Internal Auditors and in addition to the normal Audit Lead Sheet.

The Internal Auditors obtain the signature of the main auditee on the Audit Sheet, acknowledging the findings, and on each Non-Conformance Report to agree the non-conformance. A copy of the

Date Created	01/07/2018
Status	Final
Version	1.0
Review Date	01/07/2019
Owner	Data Protection Officer
Approved By	MD

Audit Sheet is given to the auditee for information and the complete report, together with all working papers, are sent to the Lead Auditor.

The Lead Auditor will file any working papers that do not form part of the official report separately.

On receipt of the completed Audit Report, the Lead Auditor logs the Audit Report, and progresses any Non-Conformance Reports through the Corrective, Preventive Action Procedure cross-referencing the Non-Conformance Report Log Number on the Audit Lead Sheet.

The Lead Auditor and relevant staff should consider formally assessing the risks presented to TRENT VALLEY ELECTRICAL SERVICES LTD of the nonconformity until it has been closed and adding them to the risk register if appropriate.

The Lead Auditor reviews the observations, with a view to raising a Non-Conformance Report relating to each issue. This then serves to address the findings without a formal non-conformance being raised at audit, and without the Audit Report remaining open for an unnecessarily extended period of time.

When all the non-conformities associated with an audit have been closed the Lead Auditor signs the Internal Audit Report Sheet as completed. A complete copy of the Audit Report is sent to the Board for confirmation of the closing of the report.

Where the Lead Auditor has reason to believe that the cause of the non-conformance may have resulted in similar non-conformances elsewhere, he/she may require follow-up audits to be carried out on that item, either in the originating area or other affected areas. These are planned in accordance with the process described above.

Should follow-up audits prove necessary, they shall be undertaken in accordance with the requirements of this procedure.

The results of audits shall be summarised by the Lead Auditor and reviewed at Management Review Meetings.

Date Created	01/07/2018
Status	Final
Version	1.0
Review Date	01/07/2019
Owner	Data Protection Officer
Approved By	MD

4. AUDIT CHECK LIST

No.	Question	Response Y/N	Comments
1	**Accountability and governance**		
1.1	Are decision makers and key people in your organisation aware that the law is changing to the GDPR and do they appreciate the impact this is likely to have?		
1.2	Is your organisation raising awareness throughout the company of any changes?		
1.3	Have areas that could cause compliance problems under the GDPR been identified and have they been recorded in the risk register?		
1.4	Have you set out the management support and direction for data protection compliance in a framework of policies and procedures?		
1.5	Does your business monitor compliance with data protection policies and regularly review the effectiveness of data handling/processing activities and security controls?		
1.6	Have you developed and implemented a needs-based data protection training programme for all staff?		
1.7	Data protection by design and default Have appropriate technical and organisational measures been implemented to show you have considered and integrated data protection into your processing activities?		
1.8	Do the organisation and staff understand when a DPIA must be conducted and are there processes in place to action this?		
1.9	Do your DPIAs account for your existing risk management and project management processes?		
2	**Designation of DPO**		
2.1	Has a data protection officer (DPO) been appointed and given responsibility for GDPR compliance and the management of organisational procedures in line with the requirements of GDPR?		
2.2	Does your organisation support the DPO by providing them and senior management with appropriate training and reporting mechanisms?		

2.3	Is there a clearly available mechanism (e.g. webpage, etc.) for data subjects that explains how to contact your organisation to pursue issues relating to personal data?		
3	**Documentation to demonstrate compliance**		
3.1	Article 30 - register of processing Have you documented your data processing activities?		
3.2	Have you included an appropriate privacy notice in each data collection process, including those via third parties?		
3.3	Have you agreed a schedule to review current privacy notices contracts for compliance with GDPR?		
3.4	Where consent is inadequate grounds for collecting and processing employees' personal data, has your organisation recorded the legal grounds on which it does so?		
3.5	Data inventory/information asset register Have you identified what personal data is collected and whether this is collected directly from the data subject or via a third party?		
3.6	Does this inventory include data retention periods, or do you have a separate data retention schedule?		
3.7	Do you have a register of data breaches and security incidents?		
4	**Processes and procedures to support compliance**		
4.1	Has you reviewed the various types of processing your organisation carries out?		
4.2	Have you have identified your lawful basis for your processing activities and documented this?		
4.3	Have you explained your lawful basis for processing personal data in your privacy notice(s)?		
4.4	Have you reviewed how you seek, record and manage consent?		
4.5	Have you reviewed the systems currently used to record consent and have you implemented appropriate mechanisms to ensure an effective audit trail?		
4.6	If your organisation offers services directly to children, have you communicated privacy information in a clear, plain way that a child will understand?		

4.7	If your organisation offers 'information society services' directly to children, do you have systems in place to verify individuals' ages and to obtain parental or guardian consent where required?		
4.8	Have you identified all the points at which personal data is collected: websites, application forms (employment and other), emails, in-bound and out-bound telephone calls, instant messaging, SMS, faxes, CCTV, exchanges of business cards and, possibly, attendance at events?		
4.9	Do you have procedures for regularly reviewing the accuracy of personal data?		
4.10	Have you identified all the ways in which personal data is stored, including backups and paper files?		
4.11	Do you have a map that clearly identifies where all this information is and how it can be accessed to meet a subject access request?		
4.12	Have you identified the purposes for processing personal data, for determining and authorising internal or external access and all disclosures of data?		
4.13	Are your organisational procedures checked to ensure that you can preserve the rights of individuals under the GDPR?		
4.14	Is there a clearly available mechanism (e.g. webpage, etc.) for data subjects that explains how to contact the organisation to pursue issues relating to personal data?		
4.15	Are all staff trained to recognise and deal with subject access requests?		
4.16	Do you have a procedure for dealing with subject access requests that will meet the requirements of the GDPR?		
4.17	Do you have a procedure for dealing with subject access requests from third parties?		
4.18	Has your organisation implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively?		
4.19	Does your organisation have mechanisms in place to assess and then report relevant breaches to the supervisory authority where the individual/data subject is likely to suffer		

	some form of damage (e.g. through identity theft or confidentiality breach)?		
4.20	Do you have mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms?		
4.21	Have you trained all staff to recognise a data breach or security incident?		
4.22	Have you trained all staff who deal with personal data about their responsibilities and data protection procedures?		
4.23	Are these responsibilities written into job descriptions?		
4.24	Do you have any automated decision-making processes (e.g. psychometric testing or credit scoring)?		
4.25	If so, do you have in place a review or appeal procedure for any customer or employee who is turned down/rejected by any automated decision software?		
4.26	Have you contracted with any third-party data processors?		
4.27	If so, do you have appropriate contracts in place with them?		
4.28	Have you agreed a schedule to review current contracts for compliance with GDPR?		
4.29	Do you transfer personal data to organisations in countries outside the EU?		
4.30	If so, do you have in place appropriate contracts and methods of ensuring compliance?		
4.31	If your organisation operates in more than one EU member state, have you determined your lead supervisory authority and documented this?		
4.32	Do you have in place adequate information systems security (e.g. as specified in ISO/IEC 27001) and does it include physical, logical, technical and operational measures that ensure the security of processing of personal data?		