GDPR AUDIT POLICY

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. PURPOSE AND SCOPE

This policy outlines the procedure for conducting internal audits to ensure adherence to TRENT VALLEY ELECTRICAL SERVICES LTD quality management system and to ensure our policies and procedures meet the requirements of external bodies.

2. RESPONSIBILITIES

Planning and the implementation of internal audits is the responsibility of the TRENT VALLEY ELECTRICAL SERVICES LTD quality person as well as recording and reporting of audits findings.

3. INTRODUCTION

Internal audits are conducted at planned intervals to determine whether processes and products:

- Conform to TRENT VALLEY ELECTRICAL SERVICES LTD quality management system and the requirements of the standards to which we are accredited
- Are effectively implemented and maintained
- To identify where improvements can be made

4. AUDIT PLAN

An audit plan shall be prepared that spans a period of 12 months. The plan will show when each part of the quality management system is to be audited. When preparing the audit plan the following should be considered:

- The status and importance of the processes and areas to be audited
- Previous audit results
- The introduction or changes to processes, methods, personnel or technology
- Where a specific need is identified, additional audits may be made, that are not part of the plan. These may be initiated at a request of TRENT VALLEY ELECTRICAL SERVICES LTD quality person or made as part of the management review process, or where new processes are introduced.

5. SELECTION OF AUDITORS

The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Where practically possible, auditors do not audit their own work.

6. AUDIT PREPARATION

Prior to an audit, the lead auditor should inform the person of the area that an audit is to take place and arrange an agreeable time. The lead auditor(s) examine the relevant documentation and records of the area or process to be audited. Documentation and records may include procedures, results and plans of previous audits, prepared checklist question, corrective actions and other quality records. Taking into account the audit scope and objectives and the information gained from the examination of the documentation and records, the lead auditor(s) prepare a checklist as a guide to conducting the audit.

7. CONDUCTING THE AUDIT

Audits start with a short meeting where the scope and objectives are agreed. When conducting the audit, the following sequence of activities should be followed:

- Establish the facts by interviewing personnel, examining documents, observing processes

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

- Under controlled conditions, examining material and equipment
- Record the facts as evidence of what took place on the audit
- Evaluate the facts to determine if there is objective evidence of non-conformity

8. AUDIT REPORTING

When the audit is complete the lead auditor:

- Writes an audit summary report
- Arranges a closing meeting
- The lead auditor will present a summary of the audit findings at the closing meeting
- Non-conformities will be reviewed and agreement obtained to timely corrective actions
- Where non-conformities have been identified, a non-conformity report will be raised

Audit reports findings are reported to the management of TRENT VALLEY ELECTRICAL SERVICES LTD and any areas for improvement are added to the risk register.

9. AUDIT FOLLOW UP

It is essential to make sure that corrective actions are taken and are effective. All non-conformities must be followed up to verify corrective actions and to complete the audit cycle. Depending on the type and severity of the non-conformity, the corrective action may be verified by:

- A limited re-audit
- A documentation review
- Verification at the next scheduled audit

The audit is completed only when all corrective actions have been verified.

10. PRIVACY AUDIT

The objective of a privacy audit is to assess TRENT VALLEY ELECTRICAL SERVICES LTD against any legislative/regulatory requirements or international best practices to ensure compliance with the General Data Protection Regulations (GPDR). Personally Identifiable Information (PII) is information that directly or indirectly identifies an individual for examples that information that could be considered PII:

- Name
- Date of Birth
- National Insurance Number
- Photographic Identifiers
- Driver’s License Number
- Biometric Identifiers (e.g., fingerprint and voiceprint, photo)
- Mother’s Maiden Name
- Vehicle Identifiers (e.g., license plates)
- Mailing Address
- Phone Numbers (e.g., phone, fax, and cell)
- Financial Account Information and/or Numbers (e.g., checking account number and PINs)
- Certificates (e.g., birth, death, and marriage)
- Legal Documents or Notes (e.g., divorce decree, criminal records, or other)
- Web URLs

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

- E-mail Address
- Education Records
- Employment Status and/or Records

Privacy is the ability of an individual to exercise control over the collection, use, and dissemination of PII. Confidentiality Assurance that PII is not disclosed to unauthorized entities (people and systems).

Value of Privacy Audits

- Measures privacy effectiveness
- Demonstrates compliance
- Reveals gaps between required and actual privacy management, operational and technical controls
- Provides basis for privacy remediation and improvement plan
- Enhances effectiveness and completeness of security assessment process by addressing privacy-specific criteria

Sample PII Risk Levels

Risk Level 1: Low risk of tangible or intangible harm if compromised – E.g., middle name, postal code. A very limited number of individuals' PII may be exposed, and/or PII is of limited sensitivity such that the exposure would cause minimal distress or inconvenience, requiring few or no corrective actions on the part of the individual and/or the program. The perception that privacy is being intruded upon is limited, and/or mitigation factors in place make the likelihood of exposure minimal.

Risk Level 2: Moderate risk of tangible or intangible harm if compromised – E.g., driver's license number. Numerous individuals' PII may be exposed; and/or PII is of sensitivity such that exposure would cause significant distress or inconvenience requiring some corrective actions on the part of the individual and/or the program. The perception that privacy is being intruded upon is likely, and/or there is a strong possibility that adverse events will occur if no additional corrective measures are taken.

Risk Level 3: High risk of tangible harm if compromised – E.g., National Insurance Number. A very large number of individuals' PII may be exposed, and/or the nature of the PII is of high sensitivity such that exposure would cause extreme distress (e.g., vulnerability to blackmail) or inconvenience (e.g., identity theft) requiring extensive corrective actions on the part of the individual and/or the program. The perception that privacy is being intruded upon is extremely likely, and/or it is nearly certain that adverse events will occur if no additional corrective measures are taken.

Steps in the Privacy Audit

- Define scope of audit and approach
- Identity stakeholders and their responsibilities
- Complete Audit Plan
- Develop audit criteria
- Used self-assessment criteria and results as starting point for developing audit criteria
- Write Audit Report and discuss remediation steps

GDPR AUDIT POLICY

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

Scope of the audit

Information security

- Tracking an individual's actions and manipulation of information
- Determining the sensitivity of derived and aggregated data
- Processes and mechanisms (e.g., authenticators)
- Ensuring that information cannot be recovered once deleted

Privacy

- Tracking the trail of PII disclosure
- Ensure that inaccurate PII is not used to make an inappropriate decision about a person
- Check new PII is and fulfills a stated purpose
- Ensuring that PII is only disclosed for a purpose consistent with the reason it was collected
- Addresses the need for the complete elimination of collected information once it has served its purpose