Introduction

Purpose of the Pack

This Board Governance, Risk & QMS Pack has been developed to provide a structured and comprehensive framework for the governance, management, and operation of the organisation.

The purpose of this pack is to:

- Establish clear governance standards and board oversight
- Ensure regulatory and legal compliance
- Support effective risk identification, management, and mitigation
- Promote financial integrity and internal controls
- Embed quality management principles and continuous improvement
- Enhance transparency, accountability, and stakeholder confidence

This pack serves as a central reference point for directors, management, employees, and relevant stakeholders, and may be used to demonstrate compliance to auditors, regulators, investors, and partners

Table of Contents

Corporate Governance

Corporate Governance and Risk Framework

Purpose

This Corporate Governance and Risk Framework establish the principles, structures, processes, and responsibilities required to ensure effective governance, ethical conduct, accountability, risk management, and regulatory compliance across the organisation.

The framework is designed to:

- Support sustainable business growth and operational resilience
- Protect stakeholders, assets, reputation, and information
- Ensure effective oversight and decision-making
- Promote compliance with applicable laws, regulations, and standards
- Embed risk awareness and accountability throughout the organisation

This document integrates:

- Governance (Section 1)
- Risk Management (Section 2)
- Compliance (Section 6)

Governance Principles

The organisation adopts the following core governance principles:

1. Accountability: Clear accountability is assigned for strategic, operational, financial, legal, and compliance responsibilities.
2. Transparency: Management decisions, financial reporting, and operational performance are communicated accurately and appropriately to relevant stakeholders.
3. Integrity and Ethical Conduct: All employees, officers, contractors, and directors are expected to act ethically, honestly, and professionally.
4. Risk-Based Decision Making: Strategic and operational decisions should consider risk exposure, controls, and potential business impact.
5. Compliance: The organisation will comply with all applicable legal, contractual, regulatory, and industry obligations.
6. Continuous Improvement: Governance, internal controls, and risk management practices will be reviewed and improved regularly.

Governance Structure

Board of Directors

The Board is responsible for:

- Defining strategic direction
- Approving governance and risk policies

- Oversight of organisational performance and risk exposure
- Ensuring adequate internal controls and compliance arrangements
- Reviewing major incidents, audit findings, and material risks
- Promoting ethical culture and accountability

Executive Management

Executive Management is responsible for:

- Implementing strategic objectives
- Managing operational and financial performance
- Ensuring effective risk management practices
- Allocating appropriate resources for compliance and security
- Monitoring key risks and mitigation activities
- Reporting material issues to leadership
- Maintaining the risk management framework
- Monitoring compliance obligations
- Coordinating risk assessments
- Supporting policy development
- Reporting on risk and compliance performance
- Facilitating internal audits and corrective actions

Department Managers/ Installation Managers / Project Managers

Managers are responsible for:

- Identifying and managing operational risks
- Maintaining effective controls within their functions
- Ensuring staff compliance with policies and procedures
- Escalating material risks and incidents
- Supporting training and awareness activities

Employees and Contractors

All personnel are responsible for:

- Complying with organisational policies and procedures
- Reporting risks, incidents, and unethical conduct
- Protecting organisational assets and information
- Participating in mandatory training and awareness programs

Risk Management Framework

Risk Management Objectives

The organisation’s risk management approach aims to:

- Identify threats and opportunities
- Reduce the likelihood and impact of adverse events
- Support informed decision-making
- Improve business resilience and continuity
- Protect customers, employees, and stakeholders

Risk Categories

Risks may include, but are not limited to:

Risk Category	Description
Strategic Risk	Risks affecting long-term objectives and business direction
Operational Risk	Risks arising from business operations, systems, or processes
Financial Risk	Risks relating to financial management, liquidity, fraud, or reporting
Compliance Risk	Risks of legal or regulatory non-compliance
Cybersecurity Risk	Risks relating to data breaches, cyberattacks, or system compromise
Information Security Risk	Risks to confidentiality, integrity, and availability of information
Reputational Risk	Risks impacting public trust or stakeholder confidence
Third-Party Risk	Risks arising from suppliers, contractors, or service providers
Health & Safety Risk	Risks affecting employee or public safety
Environmental Risk	Risks relating to environmental impact or sustainability obligations

Risk Management Process

Step 1: Risk Identification

Risks are identified through:

- Risk assessments
- Audits and reviews
- Incident reporting
- Management meetings
- Business planning activities
- Regulatory updates
- Employee feedback

Step 2: Risk Assessment

Each risk is assessed based on:

- Likelihood of occurrence
- Potential impact
- Existing controls

Residual risk exposure: A risk matrix may be used to classify risks as:

Low – Medium – High - Critical

Step 3: Risk Treatment

Risk treatment options include:

- Avoiding the risk
- Reducing the risk through controls
- Transferring the risk
- Accepting the risk within approved tolerance levels

Step 4: Monitoring and Review

Risks and controls are reviewed regularly to ensure ongoing effectiveness.

Step 5: Reporting and Escalation

Material risks, incidents, and control failures are escalated to management and leadership as appropriate.

Internal Control Framework

The organisation maintains internal controls to support:

- Accurate financial reporting
- Protection of assets
- Fraud prevention and detection
- Operational efficiency
- Regulatory compliance
- Information security

Control Types

1. Preventive Controls - designed to prevent incidents before they occur.

Examples:

- Access controls
- Segregation of duties
- Approval workflows
- Employee training

2. Detective Controls -designed to identify incidents or control failures.

Examples:

- Monitoring and logging
- Audits
- Reconciliations
- Exception reporting

3. Corrective Controls - designed to remediate issues and reduce future recurrence.

Examples:

- Incident response
- Root cause analysis
- Corrective action plans
- System recovery procedures

Compliance Management

The organisation will:

1. Maintain awareness of applicable laws and regulations
2. Conduct compliance reviews where appropriate
3. Maintain documented policies and procedures
4. Deliver mandatory training programs
5. Investigate non-compliance incidents
6. Implement corrective and preventive actions
7. Relevant compliance areas may include:
8. Data protection and privacy
9. Employment law
10. Financial regulations

11. Health and safety
12. Anti-bribery and corruption
13. Cybersecurity requirements
14. Industry-specific standards

Information Security and Cybersecurity Governance

The organisation recognises information security as a critical governance priority.

Security Objectives

- Protect confidential information
- Maintain system integrity and availability
- Prevent unauthorised access
- Ensure secure processing of data
- Support regulatory compliance

Key Security Controls

- Access management
- Multi-factor authentication
- Endpoint protection
- Security awareness training
- Backup and recovery procedures
- Incident response processes
- Vulnerability management
- Supplier security assessments

Incident Management and Reporting

All employees and contractors must report:

1. Security incidents
2. Data breaches
3. Fraud or misconduct
4. Health and safety incidents
5. Regulatory breaches
6. Significant operational disruptions

Incident Response Process

1. Detection and reporting
2. Initial assessment and containment
3. Investigation and root cause analysis
4. Escalation where necessary
5. Corrective action implementation
6. Post-incident review
7. Material incidents should be reported to senior management and regulators where legally required.

Business Continuity and Resilience

The organisation will maintain appropriate resilience and continuity measures to minimise operational disruption.

Key Components

- Business continuity planning
- Disaster recovery arrangements
- Backup procedures
- Crisis management processes
- Recovery testing and exercises
- Critical systems and business functions should have defined recovery objectives.

Third-Party and Supplier Governance

The organisation recognises that suppliers and third parties may introduce operational, legal, financial, and cybersecurity risks.

Third-Party Controls

The organisation may implement:

- Supplier due diligence
- Contractual security requirements
- Service level agreements
- Compliance assessments
- Ongoing supplier monitoring
- Access restrictions
- High-risk suppliers should be subject to enhanced oversight.

Audit and Assurance

Internal and external audits may be conducted to evaluate:

- Compliance with policies and procedures
- Effectiveness of controls
- Regulatory compliance
- Risk management maturity
- Security posture

Management is responsible for:

- Addressing audit findings (register)
- Implementing corrective actions
- Tracking remediation activities

Training and Awareness

The organisation will provide appropriate training and awareness programs covering:

- Governance responsibilities

- Risk management
- Information security
- Data protection
- Ethical conduct
- Regulatory obligations

Training participation should be monitored and recorded. Training Packs - Connecteam

Reporting and Metrics

Management should receive regular reporting on:

- Key organisational risks
- Compliance status
- Audit findings
- Security incidents
- Business continuity readiness
- Risk treatment progress
- Policy compliance

Key risk indicators (KRIs) and key performance indicators (KPIs) should be established where appropriate.

Policy Management

All governance-related policies should:

- Be documented and approved
- Be reviewed periodically
- Be communicated to relevant personnel
- Remain aligned with regulatory and business requirements

Review and Continuous Improvement

This framework should be reviewed:

- At least annually
- Following significant organisational changes
- Following major incidents
- Following regulatory changes
- Following audit recommendations

Continuous improvement activities may include:

- Control enhancements
- Process optimisation
- Technology improvements
- Additional training
- Updated governance practices

Definitions

Term	Definition
Risk	The effect of uncertainty on objectives
Control	A measure designed to manage or mitigate risk
Residual Risk	Remaining risk after controls are applied
Incident	An event that negatively impacts operations, security, compliance, or safety
Compliance	Adherence to laws, regulations, standards, and policies
Governance	The system by which the organisation is directed and controlled

Conclusion

Effective corporate governance and risk management are essential to the organisation's long-term success, operational resilience, and stakeholder trust.

This framework establishes the structure and expectations necessary to support responsible decision-making, effective oversight, compliance, and continual improvement across all areas of the organisation.

Reference: Compliance Control Register (key for controls, supporting documents and registers)

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	1.0

Corporate Governance Statement

Connect Install Ltd is committed to maintaining high standards of corporate governance to ensure ethical conduct, transparency, accountability, and long-term sustainability in all business activities. The Company recognises that strong governance is fundamental to effective risk management, regulatory compliance, and stakeholder confidence.

Governance Framework

The Company's corporate governance framework is based on the principles of:

7. Accountability: Clear accountability is assigned for strategic, operational, financial, legal, and compliance responsibilities.
8. Transparency: Management decisions, financial reporting, and operational performance are communicated accurately and appropriately to relevant stakeholders.
9. Integrity and Ethical Conduct: All employees, officers, contractors, and directors are expected to act ethically, honestly, and professionally.
10. Risk-Based Decision Making: Strategic and operational decisions should consider risk exposure, controls, and potential business impact.
11. Compliance: The organisation will comply with all applicable legal, contractual, regulatory, and industry obligations.
12. Continuous Improvement: Governance, internal controls, and risk management practices will be reviewed and improved regularly.

Governance arrangements are proportionate to the size and nature of the business and are reviewed regularly to ensure continued effectiveness.

Leadership & Management Oversight

Overall responsibility for corporate governance rests with senior management, who provide strategic direction, approve policies, and oversee operational performance. Management ensures that governance responsibilities are clearly defined and communicated throughout the organisation.

Compliance & Legal Obligations

Connect Install Ltd operates in compliance with all applicable Irish and EU legislation, including but not limited to:

- Company law and employment legislation
- Health & safety legislation
- Data protection and GDPR requirements
- Equality and accessibility legislation
- Compliance obligations are monitored on an ongoing basis, with corrective actions implemented where required.

Policies & Internal Controls

The Company has established and maintains documented policies and procedures covering key areas including:

- Health & Safety
- Data Protection & Privacy
- Whistleblowing (Protected Disclosures)

- Equality, Accessibility & Inclusion
- Ethical conduct and professional standards
- Internal controls are designed to safeguard company assets, ensure accurate record-keeping, and support effective decision-making.

Risk Management

Risks are identified, assessed, and managed through the Company's operational and management processes. Key risks—such as health & safety, regulatory compliance, data protection, and operational continuity—are reviewed regularly, and mitigation measures are implemented where necessary.

Ethical Conduct

Connect Install Ltd promotes a culture of ethical behaviour and integrity. All employees and contractors are expected to act professionally, comply with company policies, and report concerns through established reporting channels without fear of retaliation.

Stakeholder Engagement

The Company recognises the importance of engaging openly with stakeholders, including employees, clients, suppliers, and regulators. Feedback is encouraged and used to support continuous improvement and responsible business practices.

Continuous Improvement

Corporate governance arrangements are reviewed periodically to ensure they remain appropriate, effective, and aligned with business objectives, legal requirements, and recognised standards, including the principles of ISO 9001 (Quality Management) and ISO 45001 (Occupational Health & Safety).

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	2.0

Board & Director Compliance Policy / Statement

Purpose

The purpose of this policy is to set out the duties, responsibilities, and compliance expectations of the Board of Directors of Connect Install Ltd. It ensures that directors discharge their obligations honestly, lawfully, and in the best interests of the company, in full compliance with Irish corporate governance standards and the Companies Act 2014.

Scope

This policy applies to:

I. All Directors (Company & Executive) of Connect Install;
II. Any Company Secretary, board committee members, or advisers acting under board authority;
III. All subsidiaries or controlled entities where the company has governance responsibility.

Governance Principles

The organisation adopts the following core governance principles:

13. Accountability: Clear accountability is assigned for strategic, operational, financial, legal, and compliance responsibilities.
14. Transparency: Management decisions, financial reporting, and operational performance are communicated accurately and appropriately to relevant stakeholders.
15. Integrity and Ethical Conduct: All employees, officers, contractors, and directors are expected to act ethically, honestly, and professionally.
16. Risk-Based Decision Making: Strategic and operational decisions should consider risk exposure, controls, and potential business impact.
17. Compliance: The organisation will comply with all applicable legal, contractual, regulatory, and industry obligations.
18. Continuous Improvement: Governance, internal controls, and risk management practices will be reviewed and improved regularly.

Duties of Directors

Each director has both fiduciary and statutory duties, as defined in the Companies Act 2014, including the duty to:

Fiduciary Duty	Description
Act in Good Faith	Always act honestly and in the best interests of the company.
Exercise Due Care, Skill, and Diligence	Use reasonable skill and care expected from a person in that position.
Avoid Conflicts of Interest	Disclose any personal interest in company transactions and abstain from related decisions.
Exercise Independent Judgment	Make decisions based on objective assessment, not personal or external influence.

Fiduciary Duty	Description
Act Within Powers	Follow the company's Constitution and the Companies Act.
Maintain Confidentiality	Not misuse information obtained through directorship.
Ensure Compliance	Ensure company adherence to tax, legal, employment, and environmental obligations.
Not Fetter Discretion	Avoid being bound by outside commitments that limit independent decision-making.

Board Responsibilities

The Board collectively has responsibility for:

- Approving and reviewing the company's strategic direction and annual business plan.
- Overseeing financial management, ensuring adequate controls, and approving annual accounts.
- Approving governance, risk management and internal controls.
- Ensuring legal, tax, and regulatory compliance.
- Reviewing and approving policies and procedures.
- Appointing and evaluating senior management.
- Reviewing major incidents, audit findings, and material risks
- Promoting ethical culture
- Safeguarding the interests of shareholders and stakeholders

Conflicts of Interest

1. All directors must declare any conflict of interest immediately. (see Conflict of Interest Policy)
2. Declarations must be recorded in the Register of Directors' Interests.
3. Directors with conflict must recuse themselves from related discussions and decisions.
4. Gifts, hospitality, or inducements that could influence decision-making are strictly prohibited (see Anti-Bribery & Corruption Policy).

Board Meetings and Decision-Making

- The Board shall meet at least quarterly, or more frequently as required.
- Meetings must have an agenda, minutes, and record of decisions.
- A quorum must be present as defined in the company's Constitution.
- Minutes must be approved and retained for 7 years for audit and legal purposes.
- Directors should review board papers in advance and exercise independent judgment in all matters.

Corporate and Statutory Compliance

The Board ensures that the company complies with all statutory obligations, including:

Area	Compliance Requirement
Company Registration Office (CRO)	Filing of annual returns, director changes (Form B10), and financial statements.
Revenue Commissioners	Timely submission of payroll, VAT, and tax returns.
Health & Safety	Compliance with Safety, Health and Welfare at Work Act 2005.
Data Protection	Compliance with GDPR and appointment of a Data Protection Officer (DPO) where applicable.
Employment Law	Compliance with statutory leave, contracts, and employee rights.

Record Keeping

The Company Secretary (or designated officer) will maintain:

- ✔ Board Minutes and Resolutions;
- ✔ Register of Directors and Secretaries;
- ✔ Register of Directors' Interests;
- ✔ Register of Members (Shareholders).
- ✔ Register of Beneficial Ownership (RBO)
- ✔ Register of Transfers
- ✔ Register of Allotments
- ✔ Register of Charges
- ✔ Annual Return and CRO filings;

These records must be accurate, complete, and retained for at least 7 years.

Confidentiality and Data Protection

Directors must treat all company information as strictly confidential.

Disclosure of confidential information outside the company is prohibited unless authorised by the Board or required by law.

All directors must comply with the Data Protection & GDPR Policy and ensure secure handling of personal or corporate data.

Ethics and Integrity

Directors must always uphold the highest ethical standards.

Personal or family interests must not interfere with company business.

No director shall use company assets or information for personal gain.

All directors are bound by:

I. Irish Legislation
II. Governing Bodies Regulations
III. Connect Instal: Ethical Code of Practice Pack
IV. Connect Install: GDPR Library

V. Connect Install: Health & Safety Statement

Compliance Certification

Each director must annually certify that they:

1. Have complied with their duties under the Companies Act 2014;
2. Have disclosed all relevant interests or potential conflicts;
3. Have acted in the best interests of Connect Install at all times;
4. Have reviewed and approved the company's annual compliance statement (if applicable).

This certification will be documented and retained by the Company Secretary.

Board Evaluation

The Board will conduct an annual self-assessment to evaluate performance, governance effectiveness, and compliance oversight.

Findings will be reviewed by the Managing Director and used to improve board governance and effectiveness.

Policy Breaches

Breach of director duties may result in:

- ✔ Regulatory action under the Companies Act 2014;
- ✔ Personal liability for losses or penalties;
- ✔ Removal from office;
- ✔ Reporting to authorities if legal obligations are violated.

The company will act promptly and transparently on any compliance concerns.

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Acknowledgment & Declaration

Each director must sign a statement confirming that they:

- Have read and understood the Board & Director Compliance Policy;
- Acknowledge their legal and ethical duties under Irish law;
- Will act in good faith and in the best interests of Connect Install at all times; and
- Understand that breach of these obligations may result in disciplinary or legal action.
- Documentation stored and recorded reference Compliance Control Register

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	1.0

Ethics, Integrity & Transparency

Code of Conduct & Ethics Policy

Please reference 'Ethical Code of Practice Pack' for full details of company's ethics processes.

Purpose

This policy establishes the ethical standards, professional behaviour, and integrity principles expected from all employees and representatives of the organisation. It ensures that business activities are conducted ethically, responsibly, and in compliance with applicable laws and regulations.

Scope

This Code of Conduct applies to all staff, contractors, and subcontractors engaged in business activities. It outlines expected standards of behaviour in line with Irish business ethics, health & safety, and employment law.

The objectives are to ensure honesty, fairness, and professionalism in all dealings; maintain compliance with Irish legal and regulatory standards; and promote safety, sustainability, and respect for clients and colleagues.

Ethical Principles and Standards

1) Integrity and Honest Conduct

   Employees must act honestly, transparently, and responsibly in all professional activities. Decisions should be made in the best interest of the organisation and its stakeholders.

2) Compliance with Laws and Regulations All employees must comply with applicable laws, regulations, and internal policies in every location where the organization operates with Irish law, including:
   - Safety, Health and Welfare at Work Act 2005
   - Employment Equality Acts 1998–2015
   - Data Protection Acts 2018 (GDPR)
   - Criminal Justice (Corruption Offences) Act 2018
   - Companies Act 2014
   - Hold and maintain all required licenses, insurance, and professional certifications, and never engage in illegal, misleading, or unethical conduct.

Respectful and Inclusive Workplace

The organisation is committed to maintaining a workplace that is:

- respectful
- inclusive
- free from discrimination and harassment
- All employees must treat colleagues, clients, and partners with dignity and professionalism.

Please reference team policies located in the Policies under Diversity, Equity & Inclusion section in chapter 2 of the employee handbook.

Conflicts of Interest

Employees must avoid situations where personal interests could interfere with business decisions.

Potential conflicts must be disclosed to management so that appropriate measures can be taken. (see Conflict of Interest policy – Ethical Code of Practice Pack')

Examples include:

- financial interests in suppliers or competitors
- outside employment that affects work duties
- personal relationships influencing business decisions.

Anti-Bribery and Corruption

- Employees must not offer, give, request, or accept bribes or improper advantages.
- Business decisions must never be influenced by inappropriate gifts, payments, or benefits.
- Do not accept gifts or hospitality that may compromise objectivity (all gifts must be declared via gift form - Connecteam).

Confidentiality and Information Protection

Employees must protect confidential information belonging to:

i. the organisation
ii. clients
iii. suppliers
iv. employees

Confidential information must not be disclosed without proper authorisation.

Fair Business Practices

The organization is committed to fair competition and ethical business relationships with customers, suppliers, partners, and regulators.

Employees must avoid deceptive or unfair practices.

Reporting Ethical Concerns

Employees are encouraged to report any suspected:

- unethical conduct
- violations of this policy
- illegal activities
- Reports can be made through management or designated reporting channels.
- The organisation strictly prohibits retaliation against individuals who report concerns in good faith.

Health, Safety, and Environment

- Comply fully with company Health & Safety Management System and site safety requirements. Report hazards or near misses immediately.

- Use all protective equipment safely.
- Ensure installations meet or exceed regulatory standards.
- Minimise environmental impact and follow best practice guidelines.

Data Protection and Confidentiality

- Handle all data in accordance with the Data Protection Act 2018 (GDPR).
- Do not share client or company information without authorisation.
- Use company IT systems responsibly and protect proprietary materials.

Company Property and Resources

- Use company tools, vehicles, and equipment responsibly and only for work purposes.
- Report any damage or misuse immediately.
- Respect intellectual property rights and confidentiality agreements.

Responsibilities

Employees must:

- comply with this policy/all company policies.
- behave ethically and responsibly.
- report potential violations.

Management must:

- lead by example
- promote ethical culture.
- ensure employees understand the policy.

Violations

Failure to comply with this policy may result in disciplinary action, including termination of employment and possible legal consequences.

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership

Role	Responsibility
Review Frequency	Annual
Effective Date	Q2 FY27
Version	2.0

Directors' Conflicts of Interest Policy

Purpose

The purpose of this policy is to ensure that Directors act with integrity, transparency, and in the best interests of the Company at all times.
This policy provides guidance for identifying, disclosing, and managing actual, potential, or perceived conflicts of interest.

Scope

This policy applies to:

I. All members of the Board of Directors
II. Committee members of the Board
III. Any individual acting in a governance or decision-making role on behalf of the Company.

Definition of Conflict of Interest

A conflict of interest occurs when a director's personal, financial, or other interests could influence or appear to influence their decisions or actions in relation to the Company.

Examples include:

- Financial interest in a supplier or contractor of the Company
- Employment or consultancy with a competing organization
- Personal relationships affecting business decisions
- Use of company information for personal gain.

Duty of Directors

Directors must:

I. Act honestly and in good faith in the best interests of the Company
II. Avoid situations where their personal interest's conflict with those of the Company
III. Disclose any actual or potential conflicts promptly
IV. Not use their position or company information for personal benefit.

Disclosure of Conflicts

Directors must disclose conflicts:

I. Upon appointment to the Board
II. Annually through a Register of Interests
III. Immediately when a new conflict arises
IV. At the start of meetings where a conflict relates to agenda items.
V. All disclosures must be recorded in the Register of Interests maintained by the Company Secretary.

Management of Conflicts

Where a conflict is identified, the Board may decide that the Director must:

I. Abstain from discussions on the matter
II. Abstain from voting
III. Leave the meeting during discussion
IV. Provide additional information to the Board.
V. The conflicted Director must not influence the decision-making process.

Recording Conflicts

All conflicts and actions taken to manage them must be recorded in:

- Board meeting minutes
- The Company's Register of Interests.

Breach of Policy

Failure to disclose or manage a conflict of interest may result in:

- Formal warning
- Removal from Board committees
- Possible removal from the Board in accordance with the Company's constitution or governing laws.

Documents used with this policy:

Directors Declaration of Interests Form

Register of Interests

Annual Conflict Disclosure Form

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	1.0

Related Party Transactions Policy

Purpose

The purpose of this policy is to ensure that all related party transactions (RPTs) undertaken by Connect Install are conducted transparently, at arm's length, and in compliance with Irish company law and ethical business standards.

This policy safeguards against conflicts of interest, undue influence, and improper financial benefit to any related party.

Scope

This policy applies to:

- All directors, senior management, employees, and shareholders of Connect Install;
- Any related parties, as defined by the Companies Act 2014 and relevant accounting standards (FRS 102 / IAS 24);
- All transactions, whether financial or non-financial, between the company and a related party.

Legal and Regulatory Framework

This policy aligns with:

- Companies Act 2014 (Ireland) – Sections 238–241 on substantial property transactions and director interests;
- FRS 102 / IAS 24 – Related Party Disclosures;
- Corporate Governance Guidelines for SMEs in Ireland (Chartered Accountants Ireland).

Definition of a Related Party

A related party is any person or entity that has a close relationship with Connect Install or can exercise significant influence over it.

This includes:

- Directors of the company or any group company;
- Close family members of directors or key employees (e.g. spouse, partner, children, siblings, parents);
- Shareholders holding a significant ownership interest;
- Companies or entities controlled or influenced by any of the above;
- Key management personnel and their immediate family;
- Subsidiaries, joint ventures, or associates of Connect Install.

Definition of a Related Party Transaction

A Related Party Transaction is any transfer of resources, services, or obligations between Connect Install and a related party, regardless of whether consideration is exchanged.

Examples include:

- Sale or purchase of goods, services, or assets;
- Leases or property rentals;
- Loans, guarantees, or advances;
- Employment or consultancy arrangements;
- Transfer of intellectual property, equipment, or use of facilities;
- Reimbursement of personal or family expenses;
- Any transaction where influence could affect fairness or objectivity.

Guiding Principles

All related party transactions must:

- Be conducted in good faith and for legitimate business purposes.
- Occur on terms no less favourable than those available to an unrelated third party.
- Be properly disclosed, approved, and recorded.
- Avoid actual or perceived conflicts of interest.
- Be fully transparent to the Board, auditors, and (where required) the Companies Registration Office (CRO).

Approval Process

- Declaration of Interest
- Directors and key personnel must declare in writing any personal interest or connection in a proposed transaction.
- Such declarations must be entered into the company's Register of Directors' Interests.

Board Review

The Board (excluding the interested party) will review the proposed transaction for:

- Commercial justification;
- Fairness of terms; and
- Compliance with applicable laws.
- Independent Assessment
- For significant transactions (over €50,000 in value or material to the company), an independent valuation or review may be required.

Formal Approval

The transaction must be approved by disinterested directors at a properly convened Board meeting.

Where required under the Companies Act, approval must also be obtained from shareholders.

Disclosure Requirements

All related party transactions must be disclosed in the company's annual financial statements in accordance with FRS 102 / IAS 24.

FRS 102 = the UK and Ireland accounting standard ("The Financial Reporting Standard applicable in the UK and Republic of Ireland"). Section 33 covers related party disclosures.

IAS 24 = the international accounting standard "Related Party Disclosures" under IFRS.

Details should include:

- Nature of the relationship;
- Type and value of transaction;
- Outstanding balances or commitments at year-end.
- The company must also comply with Companies Registration Office (CRO) reporting obligations for substantial property transactions involving directors.

Record Keeping

All RPTs must be documented in writing and retained in the company's records for at least 7 years.

The Director of Finance will maintain:

- A Register of Related Parties;
- Copies of all approval documentation, valuations, and disclosures;
- The Register of Directors' Interests updated annually or when changes occur.

Conflicts of Interest

- Employees, managers, or directors must not participate in discussions or decisions relating to a transaction in which they have an interest.
- Conflicts must be disclosed promptly and managed according to the company's Conflict of Interest Policy.
- Failure to disclose a conflict may result in disciplinary action or removal from position.

Compliance and Monitoring

- The Finance Department and Company Secretary will monitor compliance with this policy.
- Internal or external audits may review related party transactions for accuracy, transparency, and fairness.
- Any breaches must be reported to senior management and corrective action taken promptly.

Training and Awareness

All directors and managers will receive training on recognising and reporting related party transactions.

This policy will form part of the company's governance induction for new hires and board members.

Breach of Policy

Non-compliance may result in:

- Disciplinary action, up to and including termination;
- Legal or regulatory penalties; or
- Personal liability under the Companies Act for undisclosed or improperly approved transactions.

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	1.0

Whistleblowing (Protected Disclosures) Policy & Procedure

Purpose

The purpose of this policy is to provide a clear, safe, and confidential process for employees and other workers to raise concerns about suspected wrongdoing within Connect Install.

The company is committed to maintaining an ethical, lawful, and transparent working environment. This policy ensures compliance with the Protected Disclosures Act 2014 and the Protected Disclosures (Amendment) Act 2022, which protect workers who report relevant wrongdoing from penalisation or retaliation.

Workers who make disclosures in good faith will be supported and protected under this policy.

Scope

This policy applies to:

- All employees
- Contractors and subcontractors
- Consultants
- Suppliers
- Any person performing work-related services for or on behalf of Connect Install
- It covers disclosures relating to wrongdoing within the company, by employees, or by third parties associated with the company.

What is Whistleblowing / a Protected Disclosure

Whistleblowing is the practice of reporting suspected wrongdoing or malpractice within an organisation.

A Protected Disclosure is a disclosure of information that:

- The worker reasonably believes shows wrongdoing, and
- Is made in the public interest through appropriate reporting channels.

The wrongdoing may relate to actions that have occurred, are occurring, or are likely to occur in the future.

Examples of Relevant Wrongdoing

Examples of wrongdoing that may be reported under this policy include (but are not limited to):

- Criminal offences (e.g. theft, fraud, corruption, bribery)
- Failure to comply with a legal obligation.
- Miscarriage of justice
- Endangerment of health and safety
- Environmental damage
- Misuse or mismanagement of funds
- Serious breach of company policy or ethical standards
- Concealment or destruction of evidence relating to any of the above

These matters will always be taken seriously and investigated appropriately.

Matters Not Covered by This Policy

- This policy is not intended to replace existing procedures for personal employment matters.
- The following should be raised through the appropriate company procedures:
- Complaints about terms and conditions of employment
- Personal grievances or workplace disputes
- Bullying or harassment complaints
- Discrimination complaints
- Issues relating to termination of employment.
- These matters should be addressed through the Grievance Procedure or Dignity and Respect Policy, unless they involve retaliation for whistleblowing.

Key Principles

Confidentiality - All disclosures will be handled confidentially. The identity of the person making the disclosure will be protected as far as possible.

Protection from Retaliation -Workers will not suffer dismissal, disciplinary action, intimidation, or any other detriment for making a disclosure in good faith.

Fairness -All parties involved in a disclosure or investigation will be treated fairly and impartially.

Transparency -The company will respond to credible disclosures promptly and appropriately.

Making a Disclosure

Disclosures should be made as soon as possible after the information becomes known.

Internal Reporting

In the first instance, concerns should be reported to the: Protected Disclosures Officer (PDO) - Human Resources Manager

Reports may be made:

- In writing (email or letter marked “Strictly Confidential – Protected Disclosure”)
- Verbally through a confidential meeting
- Through any secure reporting channel designated by the company

To assist the investigation, the disclosure should include:

- The nature of the wrongdoing
- Relevant dates and locations
- Names or roles of persons involved.
- Any available evidence
- Contact details of the person making the disclosure (unless anonymous)

Anonymous disclosures will be accepted and assessed, though they may be more difficult to investigate.

Procedure After a Disclosure

Acknowledgement - The company will acknowledge receipt of a disclosure within 7 days where possible.

Initial Assessment - A preliminary assessment will determine whether:

- The disclosure falls within the scope of the Protected Disclosures Act
- Further investigation is required.

Investigation

Where appropriate:

- The Protected Disclosures Officer will investigate the matter, or
- An independent investigator may be appointed.

The whistleblower will be kept informed of progress where possible, subject to confidentiality and legal obligations.

The aim is to provide feedback within 90 days of acknowledgement.

Confidentiality and Data Protection

The company will ensure that:

- The identity of the whistleblower is not disclosed without consent unless required by law.
- Information relating to disclosures is securely stored.
- Access is restricted to authorised personnel only.
- All information will be processed in accordance with the Data Protection Act 2018 and GDPR.

Protection Against Penalisation

Under the Protected Disclosures Act, it is an offence to penalise or threaten a worker for making a protected disclosure.

Examples of penalisation include:

- Dismissal or demotion
- Withholding promotion or salary increases
- Harassment or intimidation
- Unfair negative performance reviews
- Exclusion from work opportunities or blacklisting
- Bullying, harassment, or any detrimental treatment towards a colleague who has made a disclosure is unacceptable.
- Any employee found to have retaliated against a whistleblower may face disciplinary action up to and including dismissal.

External Reporting Options

If a worker feels unable to report internally, or believes their concern has not been properly addressed, they may report to an external body.

Possible reporting channels include:

Protected Disclosures Commissioner - Office of the Ombudsman
Website: www.ombudsman.ie

Other prescribed bodies include:

- Health and Safety Authority (HSA) – workplace safety matters
- Revenue Commissioners – tax or financial misconduct

- Data Protection Commission (DPC) – data protection breaches
- An Garda Síochána – criminal offences

False or Malicious Reports

- Deliberately false or malicious disclosures are not protected under the Act and may result in disciplinary action.
- However, no action will be taken against individuals who make a genuine disclosure that later proves to be mistaken.

Training and Awareness

Connect Install will ensure that:

- Employees receive training on recognising and reporting wrongdoing.
- Managers and supervisors understand how to respond to disclosures.
- Awareness of this policy is promoted through induction and internal communications.

Record Keeping

The company will maintain secure records of:

- Disclosures received
- Investigations conducted
- Outcomes and actions taken.
- Records will be kept confidentially and retained for at least 5 years in compliance with data protection requirements.

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	1.0

Risk & Business Resilience

Risk Management Policy

Purpose

The purpose of this policy is to establish a structured approach to identifying, assessing, mitigating, and monitoring risks that could affect the achievement of Connect Install's objectives.
This ensures that the company operates safely, efficiently, and in compliance with Irish legislation and industry standards.

Scope

This policy applies to:

- All business divisions, functions, projects, and operations of Connect Install;
- All employees, contractors, and management staff;
- All categories of risk — operational, financial, legal, environmental, technical, reputational, and strategic.

Objectives

The objectives of this Risk Management Policy are to:

I. Promote a proactive risk management culture across the organisation.
II. Identify potential threats and opportunities early.
III. Ensure effective controls and mitigation strategies are in place.
IV. Support informed decision-making at all levels.
V. Protect people, assets, reputation, and financial sustainability.

Legal and Regulatory Framework

This policy aligns with:

- Safety, Health and Welfare at Work Act 2005
- Companies Act 2014 (Ireland)
- Data Protection Act 2018 / GDPR
- Criminal Justice (Corruption Offences) Act 2018
- ISO 31000:2018 – Risk Management Guidelines

Definition of Risk

Risk is defined as the effect of uncertainty on objectives — it can have positive or negative consequences.
Risks may arise from internal or external sources and may impact people, assets, finances, compliance, or service delivery.

Risk Management Principles

All risk management activities must be:

- Integrated into daily operations and decision-making;

- Structured and consistent across all departments;
- Inclusive, engaging staff and contractors;
- Dynamic, adapting to changes in the business environment;
- Based on best available information; and
- Reviewed regularly to ensure ongoing relevance and effectiveness.

Responsibilities

Role	Responsibilities
Directors / Senior Management	Approve the policy, define risk appetite, and oversee company-wide risk management.
Managers / Supervisors	Identify and manage risks within their areas; maintain risk registers.
Health & Safety Officer / Compliance Manager	Support the implementation of risk assessments and ensure compliance with relevant standards.
All Employees and Contractors	Report risks, incidents, or hazards promptly; follow control procedures.

Risk Categories

Risks at Connect Install may include (but are not limited to):

Category	Example Risks
Operational	Project delays, equipment failure, poor workmanship, subcontractor issues.
Health & Safety	Workplace accidents, unsafe sites, inadequate PPE or training.
Financial	Cash flow issues, credit risks, fraud, inaccurate invoicing.
Legal / Compliance	Breach of contract, GDPR violations, non-compliance with HSA
Reputational	Poor service quality, customer complaints, social media incidents.
Cybersecurity	Data breaches, phishing, system downtime, loss of client information.
Environmental	Waste disposal issues, pollution, non-compliance with EPA standards.
Strategic	Market competition, loss of key staff, economic downturn.

Risk Management Process

The company follows a five-step Risk Management Cycle:

<u>Step 1: Identification</u>

Identify risks through:

- Site inspections, audits, and meetings;
- Incident reports and employee feedback;
- Financial and operational analysis;
- Regulatory and environmental scanning.

Step 2: Assessment

Assess each risk based on:

I. Likelihood of occurrence (Low / Medium / High);
II. Impact on operations, people, or reputation.

Risk Rating	Description	Action Required
Low	Unlikely, minor impact	Monitor periodically
Medium	Possible, moderate impact	Manage with controls
High	Likely, significant impact	Immediate mitigation and management oversight

Step 3: Control / Mitigation

Implement control measures such as:

- Policies and procedures;
- Staff training;
- Insurance coverage;
- Technical safeguards (e.g. cybersecurity, maintenance plans);
- Supplier and contractor vetting.

Step 4: Monitoring and Review

- Maintain risk register
- Quarterly reporting
- Track KRIs

Internal Control Framework- The Company maintains:

- Segregation of duties
- Approval limits
- Preventive and detective controls
- Internal audit (if applicable)

Escalation triggers include:

I. Breach of risk appetite
II. Significant incidents

Step 5: Communication and Reporting

Report all significant risks or incidents to:

- Incident Reporting (Connecteam)

- Health & Safety Helpdesk Connecteam or by emailing safety@connectinstall.ie
- Senior Management / Directors;
- External authorities, where required by law.

Level	Reports To	Frequency
Operational	Management	Monthly
Management	Risk Committee	Quarterly
Risk Committee	Board	Quarterly

Risk Appetite

Connect Install maintains a moderate risk appetite — seeking to minimise exposure to legal, financial, safety, and reputational risks, while accepting reasonable risks necessary for innovation, business growth, and customer service delivery.

The Company defines acceptable risk levels as follows:

1. Financial: Moderate
2. Operational: Low
3. Compliance: Zero tolerance

1) Financial:
   The Company maintains a moderate financial risk appetite to support sustainable growth and operational stability. The Company is willing to accept controlled financial risks associated with business expansion, investment in equipment, staffing, and new contracts, provided that:
   a. Cash flow remains sufficient to meet all operational and statutory obligations;
   b. Gross margins and profitability targets are maintained;
   c. Credit exposure to individual customers or suppliers is monitored and controlled; and
   d. Financial losses do not threaten the Company's ongoing viability or reputation.
2) Operational:
   The Company has a low to moderate operational risk appetite. The Company accepts manageable operational risks inherent in installation activities, scheduling, subcontractor management, and project delivery, where appropriate controls and supervision are in place. However, the Company has a low tolerance for:
   a. Health & safety incidents;
   b. Poor workmanship or installation failures;
   c. Significant project delays;
   d. Data loss or cybersecurity breaches; and
   e. Disruption that impacts customer satisfaction or business continuity.
3) Compliance:
   The Company maintains a low compliance risk appetite and has zero tolerance for deliberate

breaches of legal, regulatory, health & safety, tax, employment, or industry-specific obligations.

The Company is committed to complying with all applicable Irish legislation, Revenue requirements, insurance obligations, and client contractual requirements at all times.

Documentation and Record Keeping

A Risk Register will be maintained, recording all identified risks, control measures, owners, and review dates.

Records of risk assessments, safety inspections, and audits will be retained for at least 7 years.

All documentation will be securely stored and accessible for audit or regulatory inspection.

Training and Awareness

All employees will receive risk awareness training appropriate to their role.

Supervisors and managers will receive additional instruction on conducting and reviewing risk assessments.

Risk management will be incorporated into project planning, onboarding, and safety briefings.

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	1.0

Business Continuity Policy

Purpose

The purpose of this policy is to ensure that Connect Install Ltd can continue or recover critical business operations in the event of disruption, emergency, or unforeseen incident while protecting employees, customers, contractors, and business assets.

Scope

This policy applies to all employees, contractors, temporary workers, and business operations undertaken by Connect Install Ltd, including office-based and site-based activities.

Fire Procedures

Fire procedures are displayed in prominent positions, on notice boards, around the workplace. They include the identity of appointed Fire Wardens, emergency exits, the location of muster points and other procedural details. All employees must ensure that they are familiar with the emergency procedures in order to minimise the risks to life in the event of an emergency situation caused by fire.

You should familiarise yourself with all emergency escape routes, the location and types of firefighting equipment available and how to use it.

There are appointed Fire Wardens in each area of the building; it is their responsibility to instigate and coordinate the effective evacuation of the area in the event of an emergency requiring immediate evacuation. If the fire alarm sounds, you must follow their instructions.

Once the building is clear a register will be taken to ensure all employees are accounted for.

It is important to practice fire procedures to ensure that they remain effective, and practice evacuations will take place periodically. These drills should be treated seriously and as real fire emergencies by all employees.

If you have issues which will affect your ability to evacuate the building, you should inform the Fire Warden who will arrange for assistance.

If an employee discovers a fire, they should:

- raise the alarm, operate the nearest call point
- inform the responsible person of the location of the fire
- only fight a fire if you are trained or are competent to do so
- do not put yourself or others at risk by stopping to fight a fire.

If an employee hears the activation of the fire alarm, they should:

- do as instructed by Fire Wardens
- evacuate in a timely manner without delaying retrieving personal items
- do not hinder other people’s evacuation
- do not use lifts
- remain calm, walk quickly and do not run
- remain at your muster point until instructed otherwise

- do not re-enter the building until instructed by a Fire Marshal.

Bomb Scare Procedure

Upon discovery of a suspicious object, package or threat of an explosive device you must be ready to assess the risks to yourself and others in the area. Following assessment of the situation you must decide on appropriate actions and act accordingly.

Telephone Warnings - If an employee is made aware of a bomb scare by telephone, they should:

- ensure they allow the caller to deliver the full message, stay calm, do not interrupt them before engaging in conversation
- keep the caller on the phone for as long as possible whilst attracting the attention of a colleague
- inform the colleague in a discreet manner, indicating them to inform the responsible person
- take note of anything about the caller that may be useful to the authorities including accents, sex, any background noises and the type of language used
- the responsible person will instigate appropriate action with guidance from the emergency services.

Suspicious objects/packages - If an employee is the recipient of a suspicious object or a package, they should:

- evacuate people in the immediate vicinity of the device/package and ensure that no one tampers with it
- inform the responsible person of the issue immediately.

Evacuation procedure

If an evacuation is deemed to be appropriate, Fire Wardens will instigate the evacuation procedure. It is important that you listen to their instruction as the evacuation plan may change depending on the nature of the threat.

Make sure that their instructions are followed as this evacuation may have been instigated by the emergency services.

Infectious Disease Procedures

Where it is recognised by the World Health Organisation or the Government that an infectious disease creates a public health emergency, the Company will assess the risk posed to its workforce by the disease.

At all times, Government advice will be followed on managing our employees in relation to infection control, overseas travel, isolation periods and other relevant matters.

With regard to the severity of the risk, we may decide to:

- stagger start and finish times so that fewer people are together at once
- cancel non-essential overseas travel to affected areas across the world
- cancel non-essential training sessions
- deal with clients/customers by phone, email or video call

- if face to face meetings must take place, ensure that facilities are suitable to minimise the spread of infection
- deploy greater levels of flexibility including permitting employees who are usually office based to work from home.
- Employees have a role to play in ensuring that the risk of infection is kept at an absolute minimum, and must themselves stick to Government guidance in relation to overseas travel etc.

Business Continuity Management Plan (BCMP)

Our Business Continuity Management Plan outlines how we plan to continue business in a variety of circumstances which are applicable to the business, "including reasonably foreseeable emergency and disruption scenarios"

The steps below form a structured approach to ensure that in the event that key business assets are lost continuity is maintained with minimal effects on the business.

Like emergency evacuations, we will test the plans to ensure their suitability and effectiveness.

Step one - introduction

In brief, the BCMP outlines the organisation, its interested parties and how long full implementation of the plans should take to ensure loss of service or production is minimal. The introduction also outlines the aims and objectives of the plan.

Step two - roles and responsibilities

This step sets out the contact details of those who are responsible for:

- development of the plans
- operation and testing of the plans and
- those with the authority of activating and escalating the plan.
- Additionally, the process for invoking the plan is also outlined in brief. Those who may be required to put the plan in motion should be aware of this.

Step three - BCMP team

The team is made up of the key staff who will be mobilised to invoke the plans after approval from those with the authority for activation. This section contains:

- details of the team, their allocated tasks and how to contact these. Contact details should include business and home contact details
- a pre-defined location to run and coordinate business activities from
- location and contents of an emergency kit containing what is required as a minimum to ensure that business activities can be undertaken.

Step four - other contacts

The details of other key contacts who have an impact on the effectiveness of the Business Continuity Management Plan are included, examples of this could be suppliers, emergency services etc.

Step five - risk register

A register of tasks categorised by the level of impact they have on the organisation's continuity of business and safety; health and welfare will be maintained. Management will implement controls suitable to the situation and ensure that they are communicated to employees.

Step six - other information

Any other information that might be applicable in any given circumstance will be detailed, this may include utilities suppliers, councillors, provisions for communicating with employees, the media and what transport, if any will be utilised.

Step seven - action plans

Recovery plan

The recovery plan ensures that critical business activities, as identified in the risk register, can be resumed following, or during, serious damage/incident.

This may involve ensuring that employees will conduct normal working tasks from home. Alternatively, locations of any recovery sites and what the facilities allow may be set out. This can include information on:

- capacity
- parking
- welfare
- post
- meeting rooms
- disabled access
- access for employees
- transport.
- Phased return to operations

This plan sets out how quickly normal service delivery can be resumed following issues requiring the plan to be invoked. This outlines what functions should be up and running within a certain timeframe. Contractual and legal requirements will take precedence followed by the services that are required to support them.

Step eight - equipment and resources

This sets out what equipment is required either in order to work from home, or from an alternative location, and how soon it should be made available, including the number of workstations, any hardware and access to software applications.

Further considerations may be outlined within this section, including:

- diversion of telephones
- connectivity
- stationery
- back up processes

- documentation and records etc.

Step nine - testing

We will implement a plan for testing all elements of the Business Continuity Management Plan.

It will break down each element and ensure that the individual components can be mobilised, this may be broken down into role plays, desktop exercises and full drills.

Supplier / Contractor Dependency

Critical Suppliers and Contractors

The Company recognises that continuity of operations may depend on key suppliers, subcontractors, utilities providers, and service partners.

Appropriate contingency arrangements will be considered where reasonably practicable.

Tracking and reporting by Finance Department.

Recovery Priorities

Critical activities shall be prioritised for recovery based on:

Health & safety obligations

Customer commitments

Regulatory requirements

IT and communications capability

Financial impact

Operational dependencies

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27

Role	Responsibility
Version	1.0

Financial Governance & Internal Controls

Accounting Policy & Procedures

Accounting Standards

The organisation shall maintain accounting records and prepare financial statements in accordance with:

- Applicable local statutory and tax requirements.
- International Financial Reporting Standards (IFRS) or relevant local GAAP.
- Internal financial management procedures and reporting requirements.

Financial Year

The organisation's financial year shall run from 1st February to 31st January unless otherwise approved by the Board of Directors. (exception: annual leave runs as a calendar year)

Basis of Accounting

The organisation shall maintain accounts on an accrual basis unless otherwise required by applicable law.

Charter of Accounts

A standardised chart of accounts shall be maintained to:

- Ensure consistency in financial reporting.
- Facilitate budgeting and management reporting.
- Enable proper classification of income, expenses, assets, liabilities, and equity.
- Changes to the charter of accounts must be approved by the Director of Finance (DOF) and Managing Director (MD)

Revenue Recognition

Revenue shall be recognised when:

- Revenue is recognised when installation or service work is completed and invoiced to the client.
- Performance obligations have been fulfilled.
- Collection is reasonably assured.
- All revenue recognition practices must comply with applicable accounting standards.

Income Recognition

- Deposits or advance payments are recorded as liabilities until work is performed.
- Retention amounts (if applicable) are recorded separately and recognised only when conditions are met.
- Credit notes and refunds must be authorised and documented.
- Payments must be allocated against the invoice with a receipt.

Expense Recognition

Expenses shall be:

- Properly authorised.
- Supported by valid documentation.
- Recorded in the correct accounting period.
- Allocated to the appropriate cost centre or project.
- In line with expenses procedure.

Procurement and Payments

Procurement Requirements

All procurement activities must:

- Follow approved procurement procedures.
- Demonstrate value for money.
- Avoid conflicts of interest.
- Be supported by approved purchase requests and quotations where required.

Supplier Management

The Finance Department shall:

- Maintain an approved supplier register.
- Verify supplier legitimacy and banking details.
- Periodically review supplier performance and pricing.

Payment Processing

Payments shall only be processed when:

- Supported by valid invoices.
- Matched to approved purchase orders and delivery confirmations where applicable.
- Properly authorised in accordance with the Delegation of Authority Matrix.
- Electronic payments should require dual authorisation where feasible.

Cash and Banking Controls

The organisation shall maintain strict controls over cash and bank accounts including:

- Segregation of duties between payment initiation, approval, and reconciliation.
- Monthly bank reconciliations.
- Restricted access to online banking systems.
- Secure management of banking credentials.
- Prompt investigation of unreconciled items.

Payroll Controls

Payroll processing must include:

- Approved employee records and contracts.

- Verification of salary changes and bonuses. (payroll authorisation form)
- Independent payroll review prior to payment (review by DOF/MD)
- Secure handling of employee and payroll data.
- Timely remittance of payroll taxes and statutory deductions. (External Payroll Company)

Asset Management

The organisation shall maintain an asset register containing:

- Asset description.
- Asset identification number.
- Purchase date.
- Cost.
- Depreciation details.
- Custodian/location.
- Physical verification of material assets shall be conducted periodically.

Financial Reporting

The Finance Department shall prepare:

- Monthly management accounts.
- Quarterly financial reviews.
- Annual statutory financial statements.
- Budget versus actual analyses.
- Cash flow forecasts.
- Reports shall be reviewed by management and presented to the Board where appropriate.

Record Retention

Financial records and supporting documentation shall be retained in accordance with legal and regulatory requirements, typically for a minimum of seven (7) years.

Fraud Prevention

Employees must:

- Report suspected fraud or irregularities immediately.
- Avoid conflicts of interest.
- Comply with ethical and anti-bribery standards.
- Any suspected fraud shall be investigated promptly and confidentially.

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	1.0

Internal Controls / Internal Audit Policy

Internal Control Framework

The organisation shall maintain an effective internal control framework designed to:

- Protect assets and information.
- Ensure reliable financial reporting.
- Promote operational efficiency.
- Support legal and regulatory compliance.
- Detect and prevent fraud and misconduct.

The internal control framework shall include:

- Preventive controls.
- Detective controls.
- Corrective controls.
- Monitoring activities.

Segregation of Duties

Key financial responsibilities shall be segregated to reduce the risk of error or fraud.

No single individual should control all stages of a financial transaction, including:

- Requesting.
- Approving.
- Processing.
- Recording.
- Reconciling.

Where staffing limitations exist, compensating controls must be implemented.

Approval Controls

All financial commitments and transactions must:

- Be approved by authorised personnel.
- Fall within approved budgets.
- Comply with the Delegation of Authority Matrix.

Reconciliations and Reviews

The following reconciliations and reviews shall be performed regularly:

- Bank reconciliations.
- Accounts receivable reconciliations.
- Accounts payable reconciliations.
- Payroll reconciliations.
- Intercompany reconciliations where applicable.
- General ledger reviews.

All reconciliations shall be reviewed and approved by an independent individual. (External Accountant)

Access Controls

Access to financial systems, accounting records, and banking platforms shall be:

- Restricted based on job responsibilities.
- Reviewed periodically.
- Removed promptly upon employee termination or role changes.
- Strong passwords and multi-factor authentication should be used where available.

Budgetary Controls

Management shall monitor:

- Budget performance.
- Material variances.
- Forecast accuracy.
- Expenditure trends.
- Significant variances must be investigated and documented.

Compliance Monitoring

The organisation shall periodically assess compliance with:

- Financial policies.
- Regulatory obligations.
- Tax requirements.
- Contractual commitments.
- Internal procedures.

Internal Audit Function

Where applicable, the organisation may establish an Internal Audit function responsible for:

- Reviewing internal controls.
- Evaluating risk management practices.
- Assessing policy compliance.
- Conducting operational and financial audits.
- Reporting findings and recommendations.
- Internal Audit shall maintain independence from operational management.

Audit Reporting

Audit findings shall:

- Be documented formally.
- Include risk ratings and recommendations.
- Be communicated to management and/or the Board.
- Include agreed remediation actions and timelines.

- Management is responsible for timely remediation of identified issues.

Whistleblowing and Reporting

Employees and stakeholders may report concerns relating to:

- Fraud.
- Financial misconduct.
- Corruption.
- Ethical violations.
- Control weaknesses.
- Reports may be made confidentially and without retaliation.

Continuous Improvement

The organisation shall periodically review and improve:

- Internal controls.
- Financial systems.
- Policies and procedures.
- Risk mitigation measures.
- Lessons learned from audits, incidents, and reviews shall be incorporated into updated practices.

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	1.0

Delegation of Authority Matrix (DoA)

Purpose

The Delegation of Authority (DoA) Matrix establishes financial approval limits and decision-making authority to:

- Ensure accountability.
- Support effective governance.
- Prevent unauthorised commitments.
- Maintain appropriate financial oversight.

General Principles

- Authority must be exercised within approved budgets.
- Delegated authority may not be further delegated unless formally approved.
- Individuals may not approve transactions that directly benefit themselves.
- All approvals must be documented and auditable.
- Splitting transactions to avoid approval limits is strictly prohibited.

Approval Authority Matrix

Transaction Type	Employee / Manager	Department Head	Finance Manager	Managing Director	Board of Directors
Purchase Requisitions	Up to €500	Up to €5,000	Up to €20,000	Up to €50,000	Above €50,000
Supplier Contracts	Recommend only	Up to €5,000	Up to €25,000	Up to €100,000	Above €100,000
Operational Expenses	Up to budget limit	Up to €5,000	Up to €25,000	Up to €50,000	Above €50,000
Capital Expenditure	Not permitted	Up to €5,000	Up to €25,000	Up to €100,000	Above €100,000
Bank Payments	Prepare only	Approve jointly	Approve jointly	Approve jointly	Not applicable
Payroll Changes	Recommend only	Approve with process	Approve with process	Approve senior management	Board approves CEO compensation
Hiring Decisions	Recommend only	Approve within budget	Review	Approve senior hires	Approve executive hires
Write-offs / Bad Debts	Not permitted	Not permitted	Up to €10,000	Up to €25,000	Above €25,000

The organisation may amend approval thresholds based on operational size, structure, and risk profile.

Dual Approval Requirements

The following transactions should require dual approval where feasible:

- Bank transfers.
- Changes to supplier banking information.
- High-value procurement.
- Payroll releases.

- Capital expenditure.

Combination of Accounts Payable / HOD / DOF / MD

Emergency Expenditure

Emergency expenditure outside standard approval limits may be authorised by the MD or designated executive, provided:

- The expenditure is necessary to protect operations, people, or assets.
- The expenditure is documented.
- The Board or Finance Team is informed promptly.

Non-compliance

Failure to comply with this policy may result in:

- Disciplinary action.
- Withdrawal of delegated authority.
- Financial investigation.
- Legal or regulatory consequences where applicable.

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	1.0

Quality & Customer Management

Quality Assurance Policy

Purpose

The purpose of this Quality Assurance Policy is to define *Connect Install's* commitment to maintaining the highest standards of quality across all operations.

It establishes the principles, responsibilities, and framework for ensuring that all products, services, and processes meet client requirements, regulatory standards, and company objectives.

Scope

This policy applies to:

- All employees, contractors, and subcontractors working for *Connect Install*;
- All installation, maintenance, and project delivery activities;
- All offices, warehouses, and site locations under company control;
- All processes related to client service, materials, documentation, and inspection.

Policy Statement

The organisation is committed to maintaining a culture of quality, accountability, continuous improvement, and customer focus across all operations.

Quality assurance activities shall ensure that products and services:

- Meet defined specifications and requirements.
- Comply with legal, regulatory, and contractual obligations.
- Are delivered consistently and professionally.
- Support customer satisfaction and business objectives.

Roles and Responsibilities

Role	Responsibilities
Managing Director	Overall responsibility for quality assurance and continuous improvement.
HOD	Maintains QMS documentation, audits, and corrective action system.
Project Managers / Supervisors	Implement QA procedures, perform inspections, and ensure compliance on site.
Employees / Contractors	Follow approved procedures and report quality issues immediately.
Suppliers / Vendors	Must meet company-approved quality and compliance criteria.

Objectives

The objectives of this framework are to:

- The organisation shall establish measurable quality objectives including:
- Customer satisfaction targets.
- Service delivery performance standards.
- Error reduction targets.
- Response and resolution timelines.
- Compliance and audit objectives.
- Continuous improvement initiatives.
- The company's quality objectives are measurable and reviewed at least annually through management reviews and internal audits.

Objective	Measure	Target
Customer satisfaction	Client feedback forms, surveys	≥ 90% satisfaction
Defect rate	Recorded installation errors / total jobs	< 2% per quarter
On-time delivery	Jobs completed by deadline	≥ 95%
Corrective actions closure	Within 30 days	100%
Staff competency	Training matrix compliance	100% trained & certified

Quality Assurance Commitment

Connect Install is committed to:

- Delivering quality workmanship and reliable services that meet or exceed client expectations;
- Complying with ISO 9001:2015 Quality Management System (QMS) requirements;
- Ensuring compliance with Irish legal, regulatory, and industry standards;
- Continuously improving operational performance, efficiency, and customer satisfaction;
- Training and supporting staff to take ownership of quality in their daily work.

Quality Management System (QMS) Framework

Connect Install's QMS is structured around ISO 9001:2015 principles and includes:

- Quality Policy and Objectives;
- Documented Procedures and Work Instructions;
- Training and Competence Management;
- Supplier and Material Quality Control;
- Inspection, Testing, and Verification;
- Corrective and Preventive Actions;
- Management Review and Continual Improvement.

All QMS procedures are controlled documents, regularly reviewed, and version tracked.

Operational Quality Controls

To ensure quality consistency across all projects, the following QA controls are applied:

Area	Quality Assurance Measure
Pre-Installation	Project documentation reviewed and approved; materials verified against specifications.
During Installation	Supervisors conduct inspections; safety and compliance checks completed daily.
Testing & Commissioning	Verification of performance and compliance with standards (e.g., ET101, Safe Electric, manufacturer specs).
Post-Completion	Quality sign-off form completed; client walkthrough; completion certificate issued.
Documentation	Records stored in accordance with the Records Management Policy (min. 7 years).

Audits and Inspections

- Internal audits are conducted at least once per year to verify QMS compliance and effectiveness.
- Site inspections are carried out periodically by project supervisors and safety officers.
- External audits (by certification bodies or clients) are supported and managed by the Quality Manager.
- Audit findings are reviewed at Management Review Meetings.

Customer Feedback and Continuous Improvement

- Client satisfaction surveys and post-installation reviews are used to gather feedback.
- Complaints are managed under the Customer Complaints & Resolution Policy.
- Lessons learned are discussed in project review meetings and integrated into future procedures.
- Continuous improvement initiatives are tracked in the Quality Improvement Plan (QIP).

Training and Competence

- All employees must complete induction and role-specific quality training.
- Technical staff must maintain valid trade certifications (e.g., SafePass, Manual Handling).
- A Training Matrix tracks expiry and renewal dates for all mandatory qualifications.
- Regular refresher training reinforces quality, safety, and compliance standards.

Records and Documentation Control

- Quality records (certificates, test reports, inspection forms, audits) must be:

    - Accurate, complete, and legible;
    - Stored securely in paper or digital format;
    - Retained for a minimum of **7 years**.
- Document control procedures ensure that only current, approved versions are in use.

Risk assessments.

Non-Conformance Management

Any identified non-conformance or quality issue shall:

- Be documented.
- Be investigated appropriately.
- Include root cause analysis where required.
- Have corrective actions assigned.
- Be monitored until resolution.

Note: Health & Safety Hub for tracking and reporting

Supplier and Third-Party Quality

Where suppliers or contractors impact service delivery or product quality, the organisation shall:

- Assess supplier suitability.
- Monitor supplier performance.
- Address quality concerns promptly.
- Maintain approved supplier records where appropriate.

Note: Section 5 - Supply Chain & Procurement in Ethical Code of Practice Pack

Continuous Improvement

The organisation shall continuously improve its quality management processes through:

- Process monitoring.
- Quality inspections and reviews
- Audit findings.
- Customer feedback monitoring
- Incident reviews.
- Staff suggestions.
- Data analysis and reporting.
- Management reviews.
- Performance measurement.
- Corrective and preventive actions (CAPA).
- Management sets annual Quality Improvement Objectives, monitored via KPIs.
- The QMS is reviewed annually for effectiveness and relevance.

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	2.0

Customer Complaints, Resolution & Refunds Policy

Purpose

The purpose of this policy is to ensure that all customer complaints, concerns, and refund requests are handled promptly, fairly, and professionally.

It provides a structured process for resolving issues and continuously improving service quality in compliance with Irish consumer protection law and *Connect Install's* Quality Management System.

Scope

This policy applies to:

- All clients, customers, and end-users of *Connect Install* services;
- All employees, contractors, and departments involved in delivering installation, maintenance, or project work;
- All forms of feedback and complaints, whether verbal, written, or digital.
- This includes complaints about service quality, workmanship, communication, delays, billing, or aftercare.

Legal and Regulatory Framework

This policy aligns with:

- Consumer Rights Act 2022 (Ireland)
- Sale of Goods and Supply of Services Act 1980
- European Union (Consumer Information, Cancellation and Other Rights) Regulations 2013
- Data Protection Act 2018 (GDPR)
- ISO 9001:2015 Quality Management Standards

Responsibilities

Role	Responsibilities
Managing Director / Owner	Overall responsibility for policy implementation and final complaint resolution.
Customer Service / Admin Team	Receive, log, and acknowledge complaints; coordinate investigation.
Project / Operations Manager	Investigate operational or technical issues and propose corrective actions.
All Employees and Contractors	Report complaints received and cooperated in resolving them promptly.
Quality Manager (if applicable)	Monitor complaint trends and lead root-cause analysis for improvements.

Principles

All complaints will be handled according to the following principles:

1. Accessibility – Customers can raise concerns easily through multiple channels.
2. Fairness – Each complaint is treated professionally, objectively and without bias.

3. Respond to concerns promptly.
4. Confidentiality – Personal data and details are protected under GDPR.
5. Transparency – Clear information on the process and timelines is provided.
6. Resolution – Aim to resolve complaints quickly and to the customer's satisfaction/ fair and reasonable outcomes
7. Improvement – Use complaint /feedback data to identify trends and prevent recurrence

Definition of a Complaint

A complaint is any expression of dissatisfaction (oral or written) from a client or customer about:

- The quality, safety, or reliability of a service or product;
- Delays, errors, or poor communication;
- Incorrect or disputed billing;
- Behaviour of company representatives; or
- Failure to meet agreed standards or contractual terms.

Complaint Submission Channels

Customers may submit complaints via:

- ✔ Email: info@connectinstall.ie
- ✔ Phone: Office 01 685 6550
- ✔ In person: At company offices during business hours. Connect Install Limited
- ✔ Unit 2, Goldenbridge Industrial Estate, Inchicore, Dublin 8, D08 YY38
- ✔ Online: Through the company website.
- ✔ Or directly to their Project / Installation Manah=ger

Complaint Handling Procedure

Step 1 – Receipt & Acknowledgment

a. Complaint logged in the Customer Complaint Register.
b. A unique reference number assigned.
c. Customer receives written acknowledgment within 3 working days.

Step 2 – Investigation

a. Complaint reviewed by the relevant manager.
b. Investigation includes review of contracts, project documentation, communication records, and site reports.
c. Additional details may be requested from the customer.

Step 3 – Response & Resolution

a. Initial resolution or explanation provided within 10 working days of acknowledgment.
b. A response shall be provided to the customer outlining:
    i. Findings.

ii. Proposed resolution.
iii. Corrective actions where applicable.
iv. Escalation options if unresolved.
v. If unresolved, escalation to the Managing Director for review.

Step 4 – Closure

a. Once resolved, a Customer Complaint Resolution Form is completed and signed off by management.
b. The customer is notified in writing and invited to confirm satisfaction.
c. The complaint is closed only when final communication is issued.
d. Complaints shall be formally closed once:
    i. The issue is resolved.
    ii. Appropriate actions have been completed.
    iii. Documentation has been updated.

Step 5 – Continuous Improvement

a. Complaint data is analysed quarterly for recurring issues.
b. Root causes are addressed through:
    i. Staff training;
    ii. Process updates;
    iii. Supplier performance reviews.

Refund and Compensation Policy

Refunds or partial refunds may be granted where:

Refunds may be considered where:

- Services were not delivered as agreed.
- Products are defective or materially non-compliant.
- Billing errors occurred.
- Legal consumer rights apply.
- Refund decisions shall consider
- Contractual obligations.
- Applicable consumer protection laws.
- Evidence provided

Refund Procedure

1. Customer submits a written refund request with supporting evidence (invoice, photos, or correspondence).
2. The request is reviewed within 10 working days.
3. If approved, a refund will be issued by bank transfer or credit note within 14 working days of approval.

4. Where a refund is not warranted, the customer will be provided with a clear written explanation.

Refund Approval Process

Refunds shall:

- Be documented.
- Be approved by authorised personnel.
- Be processed through approved financial procedures.
- Be recorded for audit and reporting purposes.
- Refunds are issued in accordance with Irish consumer protection laws and do not affect statutory rights.

Escalation and Appeals

If a customer is dissatisfied with the outcome:

- They may appeal in writing within 10 working days of receiving the final decision.
- Appeals are reviewed by the Managing Director or an independent reviewer not involved in the original investigation.
- A written response will be issued within 10 working days of appeal receipt.

If still unresolved, the customer may refer the matter to:

- Competition and Consumer Protection Commission (CCPC)
  Website: www.ccpc.ie
- Small Claims Court (for claims up to €2,000).

Record Keeping

- All complaints and refunds are logged in the Customer Complaint Register.
- Records include:
  - Date received and resolved;
  - Nature of complaint;
  - Investigation outcome;
  - Actions taken;
  - Customer satisfaction response.
- Records are retained for 7 years under the Records Management Policy.

Confidentiality & Data Protection

- Complaint details are treated as confidential and used solely for resolution and service improvement.
- Personal data is handled in compliance with GDPR and the Data Protection Policy.

- Only authorised personnel have access to complaint files.

Training & Awareness

- All employees receive training on this policy and on customer communication skills.
- Refresher sessions occur annually or when procedures are updated.
- Complaint trends are reviewed at management meetings to enhance quality.

Monitoring & Reporting

- The Operations Manager monitors complaint statistics and provides quarterly reports to management.
- Metrics tracked include:
    - Number of complaints received;
    - Resolution time;
    - Repeat issues;
    - Customer satisfaction ratings.

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	1.0

QMS & Document Control

Quality Management System (QMS)

The organisation shall maintain a Quality Management System (QMS) designed to:

- Support operational consistency.
- Ensure compliance with applicable standards.
- Promote risk management and accountability.
- Facilitate continuous improvement.
- Maintain documented procedures and records.

QMS Documentation

The QMS shall include documented:

- Policies.
- Procedures.
- Work instructions.
- Forms and templates.
- Registers and logs.
- Records and reports.
- Corrective action records.
- Audit reports.

Document Lifecycle Management

Documents shall be managed throughout their lifecycle including:

- Creation.
- Review.
- Approval.
- Distribution.
- Revision.
- Archiving.
- Disposal.

Roles and Responsibilities

Management shall assign responsibility for:

- Document ownership.
- Approval authority.
- Version control.
- Record retention.
- Access management.
- Compliance monitoring.

Document Approval

Controlled documents must:

- Be reviewed before issue.
- Be approved by authorised personnel.
- Include version numbers and approval dates.
- Be accessible to relevant personnel.

Change Management

Changes to controlled documents shall:

- Be reviewed and approved.
- Include revision history.
- Be communicated to affected personnel.
- Replace obsolete versions promptly.

Record Retention

Quality records and controlled documents shall be retained according to:

- Legal requirements.
- Regulatory obligations.
- Contractual requirements.
- Internal retention schedules.

Internal Audits

The organisation shall conduct periodic internal audits to:

- Verify compliance with procedures.
- Assess effectiveness of controls.
- Identify improvement opportunities.
- Confirm corrective action implementation.
- Audit findings shall be documented and tracked.

Corrective and Preventive Actions (CAPA)

Where issues or non-conformities are identified, the organisation shall:

- Investigate root causes.
- Implement corrective actions.
- Monitor effectiveness.
- Prevent recurrence where possible.

Management Review

Senior management shall periodically review the QMS to assess:

- Effectiveness.
- Performance metrics.
- Audit outcomes.
- Customer feedback.
- Resource requirements.

- Improvement opportunities.

Review and Updates

This control will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	1.0

Document Control Policy

Purpose

The purpose of this Document Control Policy is to establish a structured approach for the creation, review, approval, distribution, storage, retention, protection, and disposal of documented information within the Quality Management System (QMS).

Effective document control ensures that:

- Personnel have access to current and approved documents
- Obsolete or incorrect documents are prevented from unintended use
- Records are maintained accurately and securely
- Regulatory, legal, contractual, and operational requirements are met
- Organisational knowledge is protected and preserved

Scope

This policy applies to all documented information created, received, maintained, or controlled by the organisation as part of its business operations and Quality Management System.

This includes:

- Policies
- Procedures
- Work instructions
- Forms and templates
- Records
- Contracts
- Technical documentation
- Audit reports
- Training records
- Supplier documentation
- Customer documentation
- Electronic and physical records

The policy applies to all employees, contractors, consultants, and third parties handling organisational documentation.

Objectives

The objectives of document control are to:

- Ensure documents are accurate, complete, and current
- Maintain document integrity and traceability
- Prevent unauthorised access or modification
- Support compliance with ISO standards, legal obligations, and customer requirements
- Ensure retention and secure disposal of records
- Promote consistency across organisational processes

Policy Statement

The organisation shall implement and maintain a controlled document management process to ensure that all documented information required for the effective operation of the QMS is:

- Approved prior to issue
- Reviewed and updated as necessary
- Identifiable and traceable
- Available where needed
- Protected from loss, damage, or unauthorised access
- Retained for defined periods
- Securely disposed of when no longer required

Only the latest approved versions of documents shall be used for operational purposes.

Roles and Responsibilities

<u>The Board</u>

The board is responsible for:

- Supporting effective document governance
- Ensuring adequate resources for document control
- Approving high-level policies where applicable

<u>HOD</u>

The Heads of Department are responsible for:

- Maintaining the document control process
- Managing document registers and repositories
- Ensuring document reviews are completed
- Controlling version history

- Archiving obsolete documents
- Supporting audits and compliance reviews

Department Managers

Department Managers are responsible for:

- Reviewing and approving departmental documents
- Ensuring personnel use current documents
- Identifying required updates or changes
- Maintaining department-specific records

Employees and Contractors

All personnel are responsible for:

- Using only approved and current documentation
- Following document control procedures
- Protecting confidential information
- Reporting document inaccuracies or outdated content

Document Classification

Documents may be classified according to their purpose and sensitivity.

Controlled Documents: Controlled documents are formally approved and managed under this policy.

Examples include:

- Policies
- Procedures
- Work instructions
- Quality manuals
- Templates
- Standard operating procedures

Uncontrolled Documents: Uncontrolled documents are not subject to formal update distribution controls.

Examples include:

- Informational copies
- Training handouts
- Temporary drafts

Uncontrolled documents must be clearly identified where applicable.

Confidential Documents: Documents containing sensitive or restricted information shall be protected through appropriate access controls and handling procedures.

Examples include:

- Employee records
- Financial information
- Customer data
- Security documentation
- Contractual information

Document Control Requirements

Document Creation

All controlled documents shall:

- Have a unique title and document identifier
- Include version or revision numbers
- Include approval details where applicable
- Be written clearly and consistently
- Follow approved templates where required

Review and Approval

Documents must be reviewed and approved by authorised personnel prior to release.

Review activities may include:

- Technical review
- Compliance review
- Operational review
- Quality review

Approval authority shall be defined based on document type and business function.

Document Distribution

Controlled documents shall be:

- Available to relevant personnel
- Distributed through approved systems or repositories (Connecteam / SharePoint)
- Protected against unauthorised changes

Where printed copies are used, controls should exist to ensure version accuracy.

Version Control

Document changes shall be managed through version control processes.

Version control shall include:

- Revision numbering
- Change descriptions
- Approval tracking
- Effective dates

Obsolete versions shall be archived or removed from operational use.

Document Review

Controlled documents shall be reviewed periodically or when triggered by:

- Process changes
- Regulatory updates
- Audit findings
- Organisational changes
- Incident investigations

Review frequency should be risk-based and appropriate to the document type.

Record Management

Records provide evidence of activities, compliance, and operational performance.

Record Requirements

Records shall be:

- Accurate
- Legible
- Identifiable
- Retrievable
- Securely stored
- Protected from damage or loss

Record Retention

Retention periods shall consider:

- Legal requirements

- Regulatory obligations
- Contractual obligations
- Operational requirements
- Business continuity needs

Retention schedules should be documented where appropriate.

Record Disposal

Records shall be securely disposed of when retention periods expire.

Disposal methods may include:

- Secure shredding
- Permanent deletion
- Certified destruction services

Sensitive records must be disposed of securely.

Electronic Document Management

Electronic document systems shall include controls for:

- Access management
- Backup and recovery
- Audit logging
- Version history
- Data integrity
- Availability protection

Cloud-based or third-party document systems should be assessed for security and compliance suitability.

Access Control and Security

Access to documents and records shall be restricted based on business need and role responsibilities.

Security controls may include:

- User authentication
- Permission-based access
- Encryption
- Secure storage
- Monitoring and logging

Confidential and sensitive information must be protected against unauthorised disclosure.

Change Management

Changes to controlled documents shall be:

- Reviewed and approved
- Communicated to affected personnel
- Implemented in a controlled manner
- Recorded in revision history logs

Major document changes may require retraining or process updates.

Audit and Compliance

Document control processes may be reviewed through:

- Internal audits
- External audits
- Compliance reviews
- Management reviews

Nonconformities identified during audits shall be addressed through corrective action processes.

Training and Awareness

Relevant personnel shall receive training on:

- Document control procedures
- Record handling requirements
- Use of document management systems
- Confidentiality obligations

Training records shall be maintained.

Monitoring and Continuous Improvement

The organisation shall monitor document control effectiveness through:

- Audit findings
- Document review completion rates
- User feedback
- Incident trends
- Compliance metrics

Improvement opportunities shall be implemented where appropriate.

Related Documents

This policy may be supported by:

- Records Retention Policy (GDPR Library)
- Information Security Policy (Handbook)
- Data Protection Policy (GDPR Library)
- Incident Management Procedure (H&S Hub)
- Quality Management Manual (In development)
- Change Management Procedure (In development)
- Access Control Policy (In development)

Definitions

Term	Definition
Document	Information maintained and controlled by the organisation
Record	Evidence of completed activities or results achieved
Controlled Document	A document managed through formal approval and version control
Version Control	Process used to track and manage document revisions
Retention Period	Length of time records must be maintained

Conclusion

Effective document control is essential for maintaining operational consistency, regulatory compliance, organisational knowledge, and the integrity of the Quality Management System.

This policy establishes the controls necessary to ensure documented information remains accurate, secure, accessible, and properly managed throughout its lifecycle.

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership

Role	Responsibility
Review Frequency	Annual
Effective Date	Q2 FY27
Version	2.0

Compliance, Data Protection & Digital Governance

Compliance Policy and Digital Governance Framework

Purpose

- ❖ Ensures adherence to laws, regulations, and internal policies
- ❖ Supports governance and risk frameworks (See section1)

Definition

Compliance is the process of ensuring an organization follows:

I. Laws
II. Regulations
III. Industry standards
IV. Internal policies
V. Contractual obligations

Scope

- Applies to:
- Employees
- Contractors
- Third-party suppliers
- Digital systems and data processing activities

Principles

1. Zero tolerance for breaches
2. Ethical conduct
3. Transparency

Examples

- GDPR compliance
- Health & Safety compliance
- Financial reporting compliance
- Cybersecurity compliance
- Employment law compliance
- Typical Compliance Activities
- Policy creation
- Staff training
- Audits and monitoring
- Risk assessments
- Incident reporting
- Regulatory reporting

Data Protection

Definition

Data protection focuses on safeguarding personal and sensitive information from:

- Unauthorized access
- Misuse
- Loss
- Breaches
- Corruption
- It is both a legal and operational responsibility.

Key Principles (GDPR-aligned)

- Lawfulness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Examples of Data Protection Controls

- Access controls
- Encryption
- MFA (multi-factor authentication)
- Secure backups
- Data retention schedules
- Privacy notices
- Breach response procedures
- Typical Data Types
- Customer records
- Employee data
- Financial data
- Health information
- Supplier information

Digital Governance

Definition

Digital governance is the framework for managing digital systems, technology, data, and digital operations responsibly and strategically.

It ensures:

- Technology aligns with business objectives
- Digital risks are controlled
- Data is governed properly
- Systems remain secure and compliant
- Areas Covered

- IT governance
- Cybersecurity governance
- Data governance
- AI governance
- Cloud governance
- Digital risk management
- Information management
- Core Components
- Governance structures
- Policies and standards
- Roles and responsibilities
- Decision-making authority
- Monitoring and reporting
- Risk management

How They Work Together

Area	Focus	Goal
Compliance	Following rules and regulations	Avoid legal/regulatory issues
Data Protection	Protecting personal and sensitive data	Prevent breaches and misuse
Digital Governance	Managing digital operations and technology	Strategic and secure digital control

Benefits

Organizations with strong compliance, data protection, and digital governance typically achieve:

- Reduced risk
- Better security
- Regulatory readiness
- Improved customer trust
- Better operational control
- Faster audit response
- Improved resilience

Governance Roles & Responsibilities

Role	Responsibilities
Board / Directors	Oversight and strategic governance
Heads of Departments	Regulatory compliance monitoring
Data Protection Officer (DPO)	GDPR and privacy oversight
IT Support	Technical governance and security
Department Managers	Operational compliance
Employees	Policy adherence and reporting

Regulatory Register

Regulation	Applicability	Owner	Review Frequency
GDPR	Personal data processing	DPO	Annual
Employment Law	HR operations	HR Manager	Annual
Health & Safety	Workplace safety	HOD	Quarterly
Cybersecurity Standards	IT systems	IT Support	Quarterly

Data Classification

Classification	Example	Protection Level
Public	Marketing content	Low
Internal	Operational procedures	Medium
Confidential	Financial records	High
Sensitive	Personal/special category data	Critical

Data Retention Policy

Data Type	Retention Period	Disposal Method
Employee Records	6 years	Secure deletion
Financial Records	7 years	Secure destruction
Customer Data	Contract duration + legal requirement	Secure deletion

Data Subject Rights Procedure

Procedures must support:

- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object

Data Breach Response Procedure

- Incident Response Steps
- Identify breach
- Contain incident

- Assess impact
- Notify management
- Notify regulator if required
- Notify affected individuals if required
- Record corrective actions

Breach Register

Maintain:

- Date/time
- Nature of breach
- Impact assessment
- Actions taken
- Notification status

Digital Governance Framework

IT Governance

Objectives

- Align technology with business goals
- Protect digital assets
- Ensure system availability
- Manage technology risk

Cybersecurity

- Security Controls
- MFA enforcement
- Strong password policies
- Endpoint protection
- Encryption
- Access management
- Logging and monitoring
- Patch management

Access Control

- Requirements
- Role-based access
- Least privilege principle
- Joiner/mover/leaver process
- Regular access reviews
- MFA for privileged accounts

Acceptable Use

- Employees must:
- Use systems responsibly

- Protect credentials
- Avoid unauthorized software
- Report suspicious activity
- Follow security procedures

Backup & Disaster Recovery

- Backup Standards
- Daily backups
- Encrypted storage
- Offsite/cloud redundancy
- Recovery testing

Recovery Objectives

Objective	Target
Recovery Time Objective (RTO)	4 hours
Recovery Point Objective (RPO)	24 hours

Supporting Documents

- Connect Install Policies under - IT, Confidentiality & Information Security (Handbook Chapter3)
- Connect Install GDPR Library

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	1.0

Connect Install Ltd. Accessibility Statement

Effective Date: 12th May 2026

Connect Install Ltd is committed to making our website accessible to all visitors.

1. Our Commitment
We aim to improve usability and support accessibility technologies.

2. Accessibility Features
Responsive design, readable text, and clear navigation.

3. Ongoing Improvements
We continuously review accessibility standards.

4. Feedback
Please contact us if you experience accessibility difficulties on info@connectinstall.ie or via our feedback portal.

Cookie Policy / Privacy Statement / Terms of Use

For Online Presence

Cookie Policy

Introduction

This Cookie Policy explains how Connect Install Limited uses cookies and similar technologies on our website: https://www.connectinstall.ie

This policy should be read together with our Privacy Statement and Website Terms of Use.

Non-essential cookies are only placed on your device after you provide explicit consent through our cookie management banner.

You may withdraw or amend your cookie preferences at any time.

What Are Cookies?

Cookies are small text files stored on your device when you visit a website. Cookies help websites function effectively, improve user experience, analyse website traffic, and remember user preferences.

Cookies may be:

- Session cookies (deleted when you close your browser)
- Persistent cookies (stored for a specified period)
- First-party cookies (set by our website)
- Third-party cookies (set by external providers)

Types of Cookies We Use

Cookie Type	Purpose	Legal Basis
Strictly Necessary Cookies	Required for website functionality and security	Legitimate Interest
Functional Cookies	Remember preferences and settings	Consent
Analytics Cookies	Analyse website performance and usage	Consent
Advertising/Marketing Cookies	Deliver relevant advertisements and track campaigns	Consent

Cookie Inventory

Cookie Name	Provider	Purpose	Duration
cookie consent	Website	Stores cookie preferences	12 months
_ga	Google Analytics	Website analytics	2 years

Cookie Name	Provider	Purpose	Duration
_gid	Google Analytics	User session analytics	24 hours
_gat	Google Analytics	Request throttling	1 minute

This list may be updated periodically as website technologies change.

How We Use Cookies

We use cookies to:

- Enable core website functionality;
- Improve website performance and usability;
- Analyse website traffic and visitor interactions;
- Remember user preferences;
- Improve digital services;
- Support marketing activities where consent has been provided.

Managing Your Cookie Preferences

You may:

- Accept all cookies;
- Reject non-essential cookies;
- Customise cookie preferences;
- Withdraw consent at any time.
- Most browsers also allow you to control cookies through browser settings.

Browser Management Links

Chrome: Settings → Privacy and Security → Cookies and Site Data

Firefox: Settings → Privacy & Security

Safari: Preferences → Privacy

Edge: Settings → Cookies and Site Permissions

Please note that disabling certain cookies may affect website functionality.

Third-Party Cookies

Some cookies may be placed by third-party services integrated into our website, including analytics providers and embedded content providers.

Third-party providers are responsible for their own privacy and cookie practices.

Changes to This Cookie Policy

We may update this Cookie Policy periodically to reflect legal, regulatory, or operational changes.

Updated versions will be published on this page.

Document Control

Version	Date	Approved By	Review Frequency
2.0	May 2026	Management	Annual

Privacy Statement

Introduction

Connect Install Limited is committed to protecting and respecting your privacy.

This Privacy Statement explains how we collect, use, store, share, and protect personal data when you:

- Visit our website;
- Contact us;
- Use our services;
- Engage with us commercially;
- Communicate with us electronically.

This Privacy Statement has been prepared in accordance with:

- General Data Protection Regulation (EU) 2016/679 (“GDPR”)
- Irish Data Protection Acts 1988–2018
- Applicable e-Privacy requirements

Data Controller Information

Data Controller

Connect Install Limited
Company Registration Number: 713834 - Registered in Ireland
Registered Address: Unit 2, Goldenbridge Industrial Estate, Dublin, D08 YY38
Email: dataprotection@connectinstall.ie
Website: https://www.connectinstall.ie

Personal Data We Collect

We may collect and process the following categories of personal data:

Category	Examples
Identity Data	Name, company name
Contact Data	Email address, telephone number
Technical Data	IP address, browser information, device information
Usage Data	Website interactions and analytics
Communication Data	Enquiries, emails, submitted forms

We do not intentionally collect special category personal data unless legally required and supported by an appropriate lawful basis.

How We Collect Personal Data

We may collect personal data when you:

- Visit our website;
- Submit enquiries;
- Contact us by email or phone;

- Use our services;
- Subscribe to communications;
- Accept cookies;
- Interact with us commercially.

Lawful Bases for Processing

We process personal data under one or more lawful bases under Article 6 GDPR.

Processing Activity	Lawful Basis
Responding to enquiries	Legitimate Interest
Providing contracted services	Contract
Managing legal obligations	Legal Obligation
Website analytics	Consent
Marketing communications	Consent
Business administration	Legitimate Interest

Where processing is based on legitimate interests, we ensure such interests are balanced against individuals' rights and freedoms.

How We Use Personal Data

We use personal data to:

- Respond to enquiries;
- Deliver services;
- Manage client and supplier relationships;
- Improve website functionality and performance;
- Manage cybersecurity and operational security;
- Comply with legal and regulatory obligations;
- Protect company systems and data.
- We do not use personal data for automated decision-making or profiling.
- Recruitment applications

Data Sharing

We do not sell or rent personal data.

Personal data may be shared with:

- IT and hosting providers;
- Professional advisers;
- Payment or communication providers;
- Regulatory authorities where legally required;
- Approved data processors.

All processors handling personal data on behalf of Connect Install are subject to:

- Contractual confidentiality obligations;
- Data Processing Agreements (DPAs);
- Appropriate technical and organisational security measures.

International Data Transfers

Where personal data is transferred outside the European Economic Area (EEA), we ensure appropriate safeguards are implemented, including:

European Commission adequacy decisions;

Standard Contractual Clauses (SCCs);

Appropriate security and transfer risk assessments.

Data Retention

Personal data is retained only for as long as necessary for legitimate business, legal, or regulatory purposes.

Data Type	Retention Period
General enquiries	12 months
Client records	6 years
Financial records	7 years
Recruitment records	12 months
Website analytics	26 months

Secure deletion and disposal processes are applied where appropriate.

Data Security

We implement appropriate technical and organisational security measures to protect personal data.

Security controls may include:

- Access controls;
- Multi-factor authentication (MFA);
- Encryption;
- Endpoint protection;
- Secure backups;
- Monitoring and logging;
- Vulnerability and patch management;
- Incident response procedures.

Personal Data Breaches

Where a personal data breach poses a risk to individuals' rights and freedoms, Connect Install will notify the Data Protection Commission and affected individuals where required under GDPR.

All incidents are assessed, documented, and managed through internal incident response procedures.

Your Rights

Under GDPR, you have the right to:

- Access your personal data;
- Request correction of inaccurate data;

- Request erasure of personal data;
- Restrict or object to processing;
- Request portability of personal data;
- Withdraw consent;
- Lodge a complaint with the Data Protection Commission.

Requests may be submitted to: dataprotection@connectinstall.ie

We aim to respond within one month in accordance with GDPR requirements.

Identity verification may be required before processing requests.

Children's Privacy

This website and services are not intended for children under 16 years of age.

We do not knowingly collect personal data from children.

Third-Party Links

- Our website may contain links to third-party websites.
- We are not responsible for the privacy practices or content of external websites.
- Users should review the privacy policies of third-party websites independently.

Complaints

If you are dissatisfied with how we process personal data, you may contact:

Data Protection Commission (Ireland)

Website: https://www.dataprotection.ie
Address: 21 Fitzwilliam Square South, Dublin 2, D02 RD28

Records of Processing Activities

The organisation maintains Records of Processing Activities (ROPA) in accordance with Article 30 GDPR.

Changes to This Privacy Statement

We may update this Privacy Statement periodically.

Updated versions will be published on this page.

Document Control

Version	Date	Approved By	Review Frequency
2.0	May 2026	Management	Annual

Website: Terms of Use

Acceptance of Terms

By accessing or using this website, you agree to comply with these Terms of Use and all applicable Irish laws and regulations.

If you do not agree with these terms, please discontinue use immediately.

Intellectual Property

All content; trademarks, logos, graphics, text, documents, and website materials are the property of Connect Install Limited or its licensors.

Such materials are protected under:

- Irish copyright law;
- Intellectual property legislation;
- Applicable international protections.

Permitted Use

You may:

- Access website content for lawful personal or business purposes;
- Download or print content for non-commercial internal use;
- Share links to publicly available content.

You may not:

- Copy, reproduce, distribute, or commercially exploit content without written permission;
- Misrepresent website content;
- Attempt unauthorised access to systems or data;
- Introduce malicious software;
- Conduct denial-of-service attacks;
- Use automated scraping tools without consent;
- Use the website for unlawful, harmful, misleading, or defamatory purposes.

Accuracy of Information

While we aim to ensure information is accurate and up to date, we do not guarantee completeness, reliability, or suitability for any particular purpose.

Information provided on this website does not constitute professional or legal advice.

Website Availability

We do not guarantee uninterrupted or error-free access to the website.

We reserve the right to suspend, modify, or withdraw website services without notice.

Limitation of Liability

To the fullest extent permitted by law, Connect Install Limited shall not be liable for:

- Indirect or consequential loss;
- Loss of business or profits;

- Data loss;
- Website interruption;
- Errors or omissions in website content;
- Third-party website content.
- Nothing in these Terms excludes liability for:
- Fraud;
- Death or personal injury caused by negligence;
- Any liability which cannot legally be excluded under Irish law.

User Content

Where users submit forms, feedback, reviews, or communications:

Users grant Connect Install a non-exclusive royalty-free licence to use such content for legitimate business purposes;

Users must ensure submissions are lawful and do not infringe third-party rights.

We reserve the right to remove inappropriate or unlawful submissions.

Privacy and Cookies

Use of this website is also governed by:

- Our Privacy Statement;
- Our Cookie Policy.

These documents form part of these Terms of Use.

Accessibility

Connect Install is committed to improving website accessibility and usability.

If you experience accessibility difficulties, please contact us.

Governing Law

These Terms are governed by Irish law.

Any disputes arising in connection with the website shall be subject to the exclusive jurisdiction of the Irish courts.

Contact Information

For legal or website-related enquiries:

Connect Install Limited
Unit 2, Goldenbridge Industrial Estate
Dublin, D08 YY38
Email: info@connectinstall.ie
Phone: +353 (0)1 685 6550
Website: https://www.connectinstall.ie

Document Control

Version	Date	Approved By	Review Frequency
2.0	May 2026	Management	Annual

Review and Updates

This policy will be reviewed annually or upon:

- Legislative or governance changes;
- Board structural changes; or
- Recommendations from auditors, regulators, or legal advisers.
- Any amendments must be approved by the Board and communicated to all directors.

Approval and Ownership

Role	Responsibility
Framework Owner	Risk & Compliance Lead (Human Resources Manager)
Approved By	Board / Executive Leadership
Review Frequency	Annual
Effective Date	Q2 FY27
Version	2.0

Health & Safety: Operational Compliance

Health & Safety Policy

Health & Safety General Policy Statement

Connect Install Ltd recognises that it has responsibilities under the Safety, Health and Welfare at Work Act 2005, the Safety, Health & Welfare at Work (General Applications) Regulations 2007 to 2023 (as amended) for the health, safety and welfare of our direct employees, contractors when at work and for the health and safety of other people who could be affected by our work activity. We will assess the hazards and risks they face and take action to minimise hazards and control risks to an acceptable, tolerable level.

Our managers and supervisors are made aware of their responsibilities and required to take all reasonable precautions to ensure the safety, health and welfare of our workforce and anyone else likely to be affected by the operation of our business.

This business will meet its legal obligations by providing and maintaining a safe and healthy working environment so far as is reasonably practicable. This will be achieved by:

- Providing leadership and control of identifiable health and safety risks on our premises and at every worksite.
- Consulting with our employees and workers on matters affecting their health and safety.
- Considering pre-construction information and close liaison with clients, designers and other contractors.
- Providing and maintaining safe plant and equipment.
- Ensuring the safe handling and use of substances.
- Providing information, instruction, training where necessary for our workforce, taking account of any who do not have English as a first language.
- Ensuring that all employees and contractors are competent to do their work, and where appropriate giving them suitable training.
- Preventing accidents and cases of work-related ill health.
- Actively managing and supervising health and safety at work.
- Having access to competent advice.
- Aiming for continuous improvement in health and safety performance and management by regular review and revision of this policy.
- The provision of the resource, financial and other, required to make this policy and our health and safety arrangements effective.

We also recognise:

- Our duty to co-operate and work with clients, designers, contractors and other employers, when they come onto worksites in our control, to ensure the health and safety of everyone at work; and
- The same duty of co-operation when we are working on sites under the control of others.

To help achieve our objectives and ensure our employees recognise their duties under health and safety legislation, we will also remind them of their duty to take reasonable care for themselves and for others. These duties are explained on first employment at site inductions and also set out in a Safety Handbook. This is provided to each worker; it sets out their duties and our specific health and safety rules.

This policy, our procedures and arrangements will be reviewed annually.

Signature ..... Date 11/03/2026

Position Managing Director

Peninsula, Block W, East Point Business Park, Dublin 3, D03 Y564

01 855 4861 www.peninsula-ie.com

Health and Safety Services provided by Peninsula Ireland

Peninsula Ireland offers a comprehensive range of health and safety services to businesses across the country. Their services include:

- Health & Safety Advice: Expert guidance to meet H&S rules and help prevent workplace accid ents.
- Risk Assessment Services: Comprehensive reviews and assessments to identify and mitigate r isks.
- Training and E-Learning: Certified training and e-learning courses for employees to stay safe a nd follow essential guidance.
- Templates and Reporting Tools: Ready-made templates and reporting tools to streamline hea lth and safety management.
- Consultation Services: On-site visits to identify risks and write up robust procedures.

Health & Safety Department

H&S Compliance Training Packs

Our compliance H&S Course to be completed for the employee to pass probation

1. **H&S Awareness**
2. **Manual Handling Awareness**
3. **Fire Safety Awareness**
4. **Personal Protective Equipment**
5. **Silica Awareness**
6. **Hand-arm Vibration**
7. **Electrical Safety Awareness**
8. **Accident Reporting & Investigation**
9. **Legionella Awareness**
10. **Noise Awareness**
11. **Lone Working**
12. **Asbestos Awareness**
13. **Hazardous Substances (COSHH)**
14. **Working at Height**
15. **Driving for Business**

PENINSULA

Health & Safety Help Desk Connecteam

Platform for employees to log tickets for any H&S queries or log workplace safety issues

Health & Safety Committee

Manual live with TOR, structure and yearly plan - safety@connectinstall.ie

Health & Safety Hub

Health & Safety Management System

The system is currently being developed in SharePoint to provide a structured and integrated approach to the management of:

- Incidents and investigations
- Corrective and preventive actions (CAPA)
- Risk assessments
- Competency and training management
- Inspections and audits Personal protective equipment (PPE) management

Core Registers and Operational Controls

Several key registers have been established to support the operational management of health, safety, compliance, and workforce competency.

Register	Purpose
Incident Register	Incident and injury management
Corrective Actions Register	CAPA tracking and action closure monitoring
Training Matrix	Competency and training compliance management
PPE Register	PPE issuance and tracking
Audit Register	Audit findings and compliance monitoring
Risk Register	Risk assessments and hazard identification
Inspection Register	Workplace inspection tracking

These registers provide the foundation for trend analysis, root cause identification, corrective action management, and management reporting.

🧩 HOW THESE 3 SYSTEMS WORK TOGETHER

🧱 **Integrated model:**

1. ISO 45001 Tracker
→ compliance / audit readiness

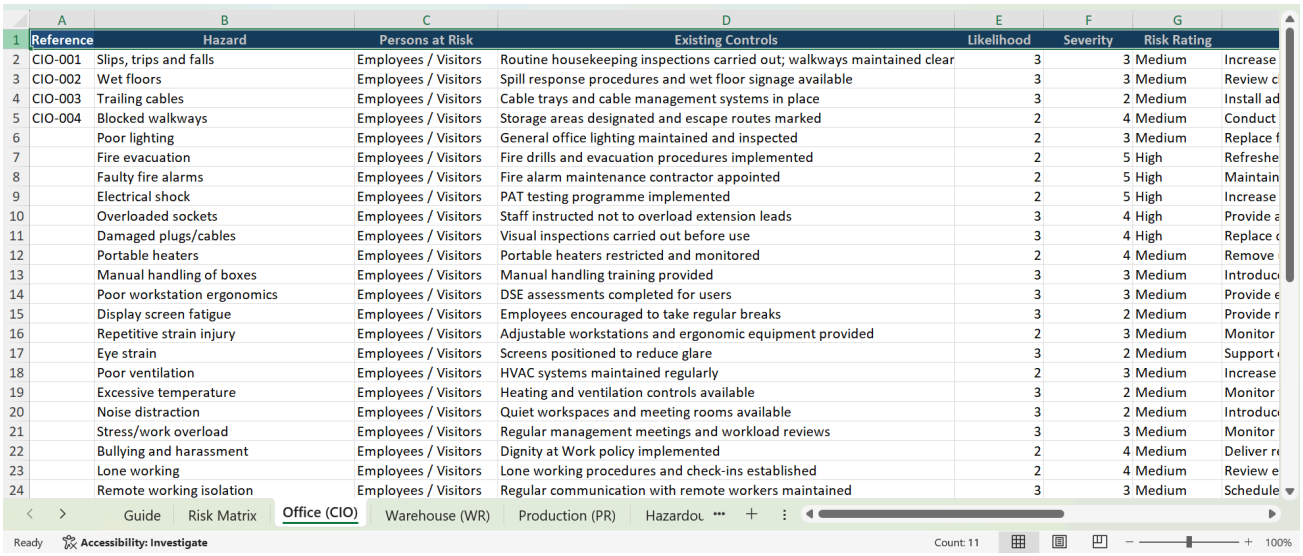
2. Incident System
→ operational safety reporting

3. KPI Dashboard

→ management reporting + forecasting

Appendices

Appendix A: Risk Register



Reference	Hazard	Persons at Risk	Existing Controls	Likelihood	Severity	Risk Rating	
CIO-001	Slips, trips and falls	Employees / Visitors	Routine housekeeping inspections carried out; walkways maintained clear	3	3	Medium	Increase
CIO-002	Wet floors	Employees / Visitors	Spill response procedures and wet floor signage available	3	3	Medium	Review c
CIO-003	Trailing cables	Employees / Visitors	Cable trays and cable management systems in place	3	2	Medium	Install ad
CIO-004	Blocked walkways	Employees / Visitors	Storage areas designated and escape routes marked	2	4	Medium	Conduct
	Poor lighting	Employees / Visitors	General office lighting maintained and inspected	2	3	Medium	Replace f
	Fire evacuation	Employees / Visitors	Fire drills and evacuation procedures implemented	2	5	High	Refreshe
	Faulty fire alarms	Employees / Visitors	Fire alarm maintenance contractor appointed	2	5	High	Maintain
	Electrical shock	Employees / Visitors	PAT testing programme implemented	2	5	High	Increase
	Overloaded sockets	Employees / Visitors	Staff instructed not to overload extension leads	3	4	High	Provide a
	Damaged plugs/cables	Employees / Visitors	Visual inspections carried out before use	3	4	High	Replace c
	Portable heaters	Employees / Visitors	Portable heaters restricted and monitored	2	4	Medium	Remove
	Manual handling of boxes	Employees / Visitors	Manual handling training provided	3	3	Medium	Introduc
	Poor workstation ergonomics	Employees / Visitors	DSE assessments completed for users	3	3	Medium	Provide e
	Display screen fatigue	Employees / Visitors	Employees encouraged to take regular breaks	3	2	Medium	Provide r
	Repetitive strain injury	Employees / Visitors	Adjustable workstations and ergonomic equipment provided	2	3	Medium	Monitor
	Eye strain	Employees / Visitors	Screens positioned to reduce glare	3	2	Medium	Support
	Poor ventilation	Employees / Visitors	HVAC systems maintained regularly	2	3	Medium	Increase
	Excessive temperature	Employees / Visitors	Heating and ventilation controls available	3	2	Medium	Monitor
	Noise distraction	Employees / Visitors	Quiet workspaces and meeting rooms available	3	2	Medium	Introduc
	Stress/work overload	Employees / Visitors	Regular management meetings and workload reviews	3	3	Medium	Monitor
	Bullying and harassment	Employees / Visitors	Dignity at Work policy implemented	2	4	Medium	Deliver r
	Lone working	Employees / Visitors	Lone working procedures and check-ins established	2	4	Medium	Review e
	Remote working isolation	Employees / Visitors	Regular communication with remote workers maintained	3	3	Medium	Schedule

Guide | Risk Matrix | Office (CIO) | Warehouse (WR) | Production (PR) | Hazardou

Ready | Accessibility: Investigate | Count: 11 | 100%

Supports risk process (*See Section 3*)

Appendix B: Calculate the Risk Rating

1. Score the Likelihood (Probability)

Estimate how likely the event is to happen. Typical 1–5 scale

Score	Likelihood	Meaning
1	Rare	Very unlikely
2	Unlikely	Could happen occasionally
3	Possible	Might happen sometimes
4	Likely	Expected to happen
5	Almost Certain	Happens frequently

2. Score the Impact (Severity / Consequence)

Estimate how likely the event is to happen Typical 1–5 scale

Score	Severity	Consequence (Injury)	Consequence (non-Injury)
1	Insignificant	Minor injury/no absence	Minimal disruption
2	Minor	First aid injury	Small operational issue
3	Moderate	Lost time injury	Noticeable business impact
4	Major	Serious injury/permanent disability	Serious financial/legal impact

5	Catastrophic	Fatality/multiple fatalities	Severe damage/business failure

3. Calculate the Risk Rating

Risk Rating = Likelihood × Impact (Severity)

Appendix C: Risk Matrix

	1 Minor	2 Medical	3 Serious	4 Major	5 Fatal
1 Rare	1	2	3	4	5
2 Unlikely	2	4	6	8	10
3 Possible	3	6	9	12	15
4 Likely	4	8	12	16	20
5 Almost Certain	5	10	15	20	25

1-5 Low [Monitor] – 6-10 Medium [Improve Controls] – 11-15 High [Action Required] – 16-25 Critical [Immediate Action]

Appendix D: Registers (Best Practice)

Corporate Governance Registers

Register	Purpose	Relevant Standard
Legal & Compliance Register	Track legal obligations and compliance status	ISO 9001 / 14001 / 45001
Policy Register	Maintain current approved policies	ISO management systems
Document Control Register	Track controlled documents and revisions	ISO 9001
Record Retention Register	Define retention periods	GDPR / ISO 9001
Company Asset Register	Track business assets	Financial / ISO
Insurance Register	Monitor insurance coverage and renewals	Best practice
Contracts Register	Track customer and supplier contracts	ISO 9001
Licenses & Certifications Register	Track operational licenses and certifications	Industry compliance
Company Vehicle Register	Manage fleet compliance	HSA / insurance
Calibration Register	Track calibrated equipment	ISO 9001

Health & Safety Registers

Required / Strongly Recommended

Register	Purpose	Standard
Risk Assessment Register	Central register of workplace hazards	ISO 45001
Accident & Incident Register	Record accidents and near misses	HSA / ISO 45001
Hazard Register	Identify operational hazards	ISO 45001
PPE Register	Track issued PPE	ISO 45001
Training & Competency Register	Employee qualifications and training	ISO 45001
Safety Inspection Register	Site and workplace inspections	ISO 45001
Tool & Equipment Inspection Register	Tool safety inspections	HSA
Fire Safety Register	Fire equipment inspections and drills	Fire Safety
First Aid Register	First aiders and incidents	HSA
Contractor Safety Register	Third-party contractor controls	ISO 45001
Permit to Work Register	High-risk work controls	ISO 45001

Information Security & GDPR Registers (ISO 27001)

Register	Purpose
GDPR Compliance Register	Data protection obligations
Data Processing Register	GDPR Article 30 requirement
Data Breach Register	Security incidents
IT Asset Register	Devices and systems
User Access Register	Access permissions
Password / Access Control Register	Security administration
Software License Register	Software compliance
Attendance Register	Workforce attendance
Timesheet Register	Labor records

Financial & Commercial Registers

Register	Purpose
Invoice Register	Customer invoicing
Accounts Payable Register	Supplier payments

Register	Purpose
Accounts Receivable Register	Debtor management
Expense Register	Company expenses
Budget Register	Financial monitoring
Insurance Claims Register	Claims management
Tender Register	Bid tracking

HR & Employee Registers

Register	Purpose
Employee Register	Staff records
Training Matrix	Competency overview
Annual Leave Register	Leave management
Disciplinary Register	HR actions
Grievance Register	Employee complaints
Recruitment Register	Hiring records
Performance Review Register	Appraisals
Right to Work Register	Employment compliance
Medical Surveillance Register	Occupational health
Driving License Register	Vehicle compliance

ISO 9001

- Internal Audit Register
- NCR Register
- Corrective Action Register
- Supplier Register
- Calibration Register
- Training Register
- Customer Complaints Register

ISO 45001

- Risk Assessments
- Incident Register
- PPE Register
- Training Register
- Safety Inspections
- Contractor Controls

ISO 27001

- Asset Register
- Access Register
- Incident Register
- Risk Register
- Backup Register

Core Registers

- Legal & Compliance Register
- Risk Assessment Register
- Training Register
- Incident Register
- Asset Register
- Insurance Register
- Supplier Register
- Corrective Action Register
- Audit Register
- Calibration Register
- Vehicle Register
- GDPR Register
- Waste Register
- Project Register
- Customer Complaints Register

Recommended Structure

Most companies organise registers under:

1. Governance
2. Quality
3. Health & Safety
4. Environmental
5. Information Security
6. Operations
7. HR
8. Financial
9. Projects
10. Compliance

Recommended File Structure

/Company-management-system
/01-Governance
/02-Quality
/03-Health-Safety
/04-Environmental
/05-GDPR-IT
/06-Operations
/07-HR
/08-Finance
/09-Projects
/10-Register