Company
LJR Group Services Limited

Version	Review date	Reviewed by	Role
1.0	12th January 2025	Shaun Radcliffe	Director
	To be Reviewed date	**Signature**	**Notes**
	12th January 2026	S A RADCLIFFE	Version 1.0

Risk Management Policy

1. Introduction

This document details LJR Group Services Ltd (Company) procedure for assessing and managing our business, including its Strategic, Financial, Regulatory Compliance, Operational, quality, environmental, health and safety, data security and GDPR risk, in line with ISO/IEC 31000 Risk Management Principles & Guidelines, specific legislation and industry standards. Our risk assessments inform strategic decisions, training, Business Continuity Procedures and Plans.

Table of Contents.

2. Purpose of Document

Company will consider all risk (Harm, Opportunity or Threat) involved in their business, their regulatory, legal and moral duties in their evidence-based decision making. Our risk management approach is set within the context of our business, the inherent risks, our appetite for and tolerance to risk.

An evidence-based decision-making process and sound risk management process ensures that an organization manages its risk consistently by establishing a repeatable process and appropriately, by ensuring that the cost of mitigating (or reducing) the particular risk can be justified when considering the consequence of accepting the risk.

The purpose of this document is to provide a description of the risk management framework which sets the context for an organization's risk assessment methodology. Specifically, this document will cover:

- The risk management framework including the organization's business context, inherent risks, the organisation's risk appetite, an established risk policy, responsibilities and authority, the need to assess risks at all levels within an organization's risk-based decisions-making and the criteria for risk acceptance.
- The risk assessment procedure to ensure that the organization establishes repeatable assessments and continually improves its processes and procedures for the identification, analysis, evaluation, treatment and residual risk acceptance.
- This risk assessment procedure also includes the procedure for undertaking risk assessments for Health & Safety and Environmental risk. The Risk assessments will be separate documents for Quality, Environmental risks and Health and Safety risks. Separate ratings charts are included in this procedure.

3. Risk Management Policy - Policy Statement.

Company will manage risk (risk should be read as including Harm, Opportunity and threats), effectively and consistently in all aspects of its business including planning, delivering, operating and overseeing programmes and performance. All management levels will develop and encourage a culture of well-informed risk-based decision making.

Commitments – Company shall be a company that:

- Makes risk management a part of strategic and tactical decision making such that whenever there are risks that could significantly affect company operations, projects and programmes, resources are deployed proportional to these risks and safety, environmental risks are managed. Maintains a current risk appetite and tolerance stance and communicates this across the company and makes decisions about operations and projects consistent with that statement.
- Establishes and maintains companywide procedures, practices and processes to ensure compliance with applicable standards and contractual provisions and remain consistent with other entities with similar risks.
- Provides clearly defined and documented accountabilities for risk management, with risks being managed at the lowest level at which the manager has the authority, responsibility and resources to take effective action.
- Ensures risks are managed in an integrated way across all levels of the organisation covering the key interdependencies i.e. strategic, programme, project and operational risk.
- Develops and maintains a core competency in risk management and has a robust continuous improvement and learning culture, that learns from internal and external experience, assesses our performance against high standards and supports personnel growth and development.
- Requires the involvement of all members of 'management'
- Ensures effective assurance arrangements are in place to monitor the effectiveness of the risk management processes on a routine basis.
- Regular reviews and updates of risks facing the business and how they are being mitigated and ensures that these are visible at the highest levels in the company.
- Incorporates credible risks in the Corporate Plan and all significant planning efforts.
- Benchmarks our risk management processes to recognised good practices, guidelines and standards and incorporates lessons learnt from inside and outside of the business.

This policy statement and risk appetite and tolerance stance will be reviewed annually.

4. Executive Summary

Business and Quality

This organizations faces inherent risks of doing business, these risks can be internal or external, more often a combination of both.

As part of good corporate governance, this organization manages risks at all levels across their business. This organization considers the potential for risks to affect the achievement of its strategic objectives and how risks can influence strategic decision making.

From an operational perspective, this organization has considered risks that have the potential to impact its operational performance and efficiency level, and from a project perspective, risks are managed to ensure that they do not affect the project outcomes and business case.

All decision making within the organization involves consideration of risks and has been in a consistent and repeatable manner. The risk management approach is an integrated part of the organization's governance for the risk management framework to be effective.

The ISO31000:2009 Risk Management standard "… recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance strategy and planning, management, reporting processes, policies, value and culture".

For the risk management to be appropriate, it has been set within the context of the organization's business context, inherent risks, the organization's risk appetite, an established risk policy and well-defined responsibilities and authority (i.e. risk management framework). For the risk management to be effective, it must be consistent, repeatable, underpinned by well-defined processes and procedures and continually improved (i.e. risk assessment processes and procedures).

Monitor, Review and Continual Improvement.

Business Risk is controlled through our Risk Register (MSF303), whereas Quality Risk is managed on MSF24. Both are considered and continually improved via our Management Review Meetings.

Health and Safety

Purpose

To determine Training needs and minimise risk associated with:

- Our work on individuals, our clients and public
- Individual projects taken on by our staff
- Generic tasks method of work
- To meet the requirements of the following:
  - Contract Conditions Safety (Various clients)
  - Health and Safety at Work Act 1974
  - ISO45001:2018
  - Any other relevant legalisation.

Scope

All projects, generic maybe used for maintenance purposes and site specific for projects.

Responsibility

It is the Managing Directors to ensure that this procedure is implemented and maintained.

Records

Risk assessments recorded on form MSF 24
All assessments to be kept with job files, projects safety files, on site and electronically at the office

Authorised persons
Only authorised persons may complete these risk assessments. Persons can only be authorised if they have completed a suitable safety-training course such as the safety foundation course, risk management course, NEBOSH, IOSH.

Monitor, Review and Continual Improvement.
Corporate Safety Risk and task procedure is considered and continually improved via our Management Review Meetings.

Individual Project risk assessments are monitored and continually improved via the Safety Officer. Performance relating to project risk assessments is discussed within our Management Review Meetings.

Environmental
Purpose

- To determine Training needs and minimise risk associated with:
- Our Environmental impact of our work.
  - Contract Conditions Environnemental
  - Environmental protection act
  - Any other relevant legalisation.

Scope
All projects, generic maybe used for maintenance purposes and site specific for projects.

Responsibility
It is the Managing Directors to ensure that this procedure is implemented and maintained.

Records
Risk assessments recorded on form MSF 15
Aspects and impacts register MSF08
All assessments to be kept with job files, projects safety files, on site and electronically at the office

Authorised persons
Only authorised persons may complete these risk assessments. Persons can only be authorised if they have completed a suitable Environmental-training course such IEMA, EMA approved training courses.

Monitor, Review and Continual Improvement.
Corporate Safety Risk and task procedure is considered and continually improved via our Management Review Meetings.

5. Risk Management Framework

5.1 Risk Appetite & Tolerance Statement/Stance

Our Risk Assessment, analysis, evaluation and treatment stance is set out in section 6 of this document.

5.2 Responsibility, Authority & Stakeholders

The executive management board has ultimate responsibility for effective risk management across the organization. The executive management board will delegate authority throughout the organization but will also retain responsibility. The executive management board will endorse and demonstrate commitment to their risk management policy and monitor performance indicators for internal and external stakeholders as well as legal and regulatory compliance.

5.3 Integration

Risk management operates at all levels within the organization in an integrated manner to be effective. Risk management is considered at a strategic, operational and project level – and considers both internal and external factors (i.e. horizontally and vertically). Risk management processes and procedures are integrated part of the organization's business. Good corporate governance requires effective risk management down and across the organization.

5.4 Risk Evaluation Criteria

The organization defines the criteria to be used to evaluate the significance of risks; this are defined to lead to consistent results and be subject to continuous review and improvement. A few factors will influence the organizations criteria for evaluating risks (e.g. likelihood, consequence, nature of the impact, reputational damage, revenue impacting, external factors etc.).

5.5 Risk Acceptance (Residual Risk)

The organization will often decide to accept risks based on due considerations such as the cost to mitigate is too high, the likelihood is low and the consequences are acceptable, the reward is worth the risk (risk versus reward) or cost of doing entering new markets.

5.6 Internal and External Factors

The organization will carefully consider the interest of both internal and external factors in their risk management approach. Such factors include customers, suppliers, competitors, stakeholders, shareholders, their products and services, their employees, legislation and regulation. The organization will consider risks to and risk arising from various internal and external factors.

5.7 Continuous Improvement

Continuous improvement will be an integral part of the risk management approach. The executive management board will typically set high-level targets and goals which will be owned by the operational functions / departments that will capture and report on metrics that contribute to the high-level targets and goals. To identify and implement improvements, the organization will monitor and measure its achievement of performance targets.

5.8 Reporting & Communication

The organization is reports and communicates internally and often externally on its risk management to demonstrate effective governance, to provide confidence that it is managing risks in accordance with its policy and for legal and regulatory compliance.

6. Risk Assessment Procedure

The Company performs a review of risks and undertakes risk assessments on a regular basis at least once a year or if circumstances should change and when there is a significant change at strategic, operational or project level.

6.1 Risk Identification

During risk identification, the Company has considered all eventualities that could have an impact on the achievement of a stated objective or plan. At a strategic level, the Company has considered the events that would impact the achievement of its strategic intent (e.g. political uncertainty, competitors, labour market skills shortage, delays in product launch, becoming the target of a hostile acquisition, cyber security threats etc.) associated with the loss of confidentiality, integrity and availability for information within the scope of the management system.

At an operational level, the Company has considered the events that would impact its achievement of production targets, quality sign-off, product launch, new IT system implementation or change programme.

At project level, the Company has considered the events that would impact the achievement of planned initiatives.

During the risk identification stage, the Company has identified and documented a comprehensive list of risks; the Company has defined the most appropriate method to achieve this end. The organization has chosen the most appropriate method for identifying risks, although this may vary depending on whether risks are being identified at a strategic, operational or project level. The Company has chosen to identify risks against their assets and to hold risk management workshops with a multi-discipline representation. The Company has also identified the owner of any identified risk as part of this process.

However, the Company decides to go about this process, the output from the risk identification will be a comprehensive set of risks, with associated impact(s), events (or cause) that could give rise to the risk and the consequence. The impact and consequence will be rated according to a 5X5 matrix using a rating chart or quantified, if possible, to do so at this stage. The output from the risk identification stage is typically documented in a risk register.

6.2 Risk Analysis

The Company's approach for risk analysis is systematic and repeatable so that the relative significance and importance of risks can be assessed. The output from the risk identification stage forms the input to the risk analysis stage.

The purpose of the risk analysis is to develop a qualitative and / or quantitative assessment of the risk so that the Company can judge the relative significance and priority of risks. During the risk analysis stage, the appropriate persons with the relevant subject matter, process knowledge and authority will be involved. The risk analysis stage involves gaining an in-depth understanding of the characteristics of the risk, in particular the impact, consequences, likelihood and relationships between risks (i.e. multiply effect). The output from this stage is a risk assessment, whereby risks are scored based on an analysis of their impact, consequence and likelihood.

6.3 Risk Evaluation

The output from the risk analysis forms the input to the risk evaluation stage. The purpose of the risk evaluation is to consider risks within the context of the Company's risk appetite and risk evaluation criteria which are defined as part of the risk management framework. The Company will make decisions about whether to treat and the priority for treatment of risks. The responsible and or authorised persons will be involved in the risk evaluation decision making.

6.4 Risk Treatment

The organization's decision on risk treatment is based on risks versus reward and the business case benefits are also considered. The output from the risk evaluation provides input to the risk treatment considerations. Depending on the type of risk and its significance to the business, the decision makers may choose to:

- Avoid – the Company may choose not to implement certain activities or processes that would incur the risk (i.e. eliminate the risk by eliminating the potential cause).
- Mitigate – to reduce the likelihood or impact of the risks by implementing appropriate mitigating controls.
- Transfer – to share the risk with a partner or transfer via insurance coverage, contractual agreement or other means.
- Accept – formally acknowledge and sign-off acceptance of the risks

6.5 Residual Risk

Even after risk treatment, is mitigated or transferred there may still exist a degree of risk which is known as the residual risk. The decision makers ensure that they understand the extent of the residual risks remaining after treatment and this is be documented, accepted, monitored and reviewed on a regular basis at least once a year.

6.6 Monitoring and Review

As an integral part of the risk management process, the Company regularly reviews, monitors, reports and communicates internally and as appropriately externally on the outcomes and effectiveness of the risk management process.

6.7 Continuous Improvement

The Company identifies opportunities for improvement, so that the risk assessment outcomes continue to be appropriate, relevant and effective.

BUSINESS & QUALITY RISK RATING CHART

Assess each individual risk for the task and enter the score on the Task Risk Assessment sheet. Multiply each score and enter the result in risk rating column. Add together each total to give final risk rating total.

Likelihood

SCORE	PROBABILITY OF EXPOSURE	CONTACT WITH HAZARD
0	IMPOSSIBLE	CANNOT HAPPEN
1	ALMOST IMPOSSIBLE	POSSIBLE UNDER EXTREME CONDITIONS
2	HIGHLY UNLIKELY	THOUGH CONCEIVABLE
3	UNLIKELY	COULD HAPPEN
4	POSSIBLE	COULD HAPPEN BUT UNUSUAL
5	EVEN CHANCE	COULD HAPPEN

Consequence

SCORE	IMPACT	FINANCE/DAMAGE LOSS
0	NO RISK OR IMPACT	NO FINICAL RISK
1	VERY LOW RISK IMPACT	5% possible finical loss
2	LOW RISK IMPACT	6-10% possible finical loss
3	MEDIUM/HIGH RISK IMPACT	11-20% possible finical loss
4	MEDIUM RISK/IMPACT	21-25% possible finical loss
5	HIGH RISK/IMPACT	26% possible finical loss

Action Table

SCORE	ACCEPT RISK/CONSIDERED ACTION
0 –9	MINOR, NO FURTHER ACTION
10 – 19	MEDIUM RISK CONSIDER CONTROLS
20 – PLUS	HIGH RISK CONTROLS REQUIRED

RATING FOR ENVIRONMENTAL RISK ASSESSMENT CHART

Assess each individual environmental risk for the task and enter the score on the Environmental risk Assessment sheet. Multiply each score and enter the result in risk rating column. Add together each total to give final risk rating total.

Likelihood

SCORE	PROBABILITY OF EXPOSURE	CONTACT WITH HAZARD
0	IMPOSSIBLE	CANNOT HAPPEN
1	ALMOST IMPOSSIBLE	POSSIBLE UNDER EXTREME CONDITIONS
2	HIGHLY UNLIKELY	THOUGH CONCEIVABLE
3	UNLIKELY	COULD HAPPEN
4	POSSIBLE	COULD HAPPEN BUT UNUSUAL
5	EVEN CHANCE	COULD HAPPEN

Consequence

SCORE	ENVIRONMENTAL IMPACT	FINANCE/DAMAGE LOSS
0	NO POSSIBLE IMPACT TO THE ENVIRONMENT	£ - TIME REMOVES RISK CONTAMINATION
1	VERY LOW IMPACT TO THE ENVIRONMENT	UP-TO £2,499.00; MINOR CLEAN UP
2	LOW IMPACT TO THE ENVIRONMENT	UP-TO £6,499.00; MEDIUM CLEAN UP
3	MEDIUM TO THE ENVIRONMENT	UP-TO £15,499.00; MAJOR CLEAN UP
4	HIGH IMPACT TO THE ENVIRONMENT	UP-TO £25,000.00; PERMANENT DAMAGE
5	SEVERE IMPACT TO THE ENVIRONMENT	PLUS & £50,000.00; PERMANENT DAMAGE

Action Table

SCORE	ACCEPT RISK/CONSIDERED ACTION
0 –9	MINOR, NO FURTHER ACTION
10 – 19	MEDIUM SOME MONITORING MAYBE REQUIRED
20 – PLUS	HIGH MONITORING REQUIRED

HEALTH & SAFETY RISK RATING CHART

Assess each individual risk for the task and enter the score on the Task Risk Assessment sheet. Multiply each score and enter the result in risk rating column. Add together each total to give final risk rating total.

Likelihood

CORE	PROBABILITY OF EXPOSURE	CONTACT WITH HAZARD
0	IMPOSSIBLE	CANNOT HAPPEN
1	ALMOST IMPOSSIBLE	POSSIBLE UNDER EXTREME CONDITIONS
2	HIGHLY UNLIKELY	THOUGH CONCEIVABLE
3	UNLIKELY	COULD HAPPEN
4	POSSIBLE	COULD HAPPEN BUT UNUSUAL
5	EVEN CHANCE	COULD HAPPEN

Consequence

SCORE	PEOPLE	FINANCE/DAMAGE LOSS
0	MINOR INJURY NO LOST TIME	£ - TIME REMOVES RISK CONTAMINATION
1	MINOR INJURY LOST TIME OCCURRENCE	UP-TO £2,499.00; MINOR CLEAN UP
2	BREAK MINOR BONE OR MINOR ILLNESS	UP-TO £6,499.00; MEDIUM CLEAN UP
3	BREAK MAJOR BONE OR MINOR ILLNESS	UP-TO £15,499.00; MAJOR CLEAN UP
4	LOSS OF LIMB, EYE, SERIOUS PERMANENT ILLNESS	UP-TO £25,000.00; PERMANENT DAMAGE
5	FATALITY	PLUS & £50,000.00; PERMANENT DAMAGE

Action Table

SCORE	ACCEPT RISK/CONSIDERED ACTION
0 –9	MINOR, NO FURTHER ACTION
10 – 15	SIGNATURE REVIEW TO LOWER SCORE
16-25	CRITICAL STOP ACTIVITY

8. INFORMATION SECURITY AND PRIVACY (INC GDPR) RISK ASSESSMENT.

Purpose

The purpose of this procedure is to detail the method used to populate and risk rate the information security Register, considering the statement of applicability and the scope of the organisation. It also serves to provide the risk rating, control measures and residual risk remaining following the application of the control measures and agreed by the information security management representative.

Identify assets and ownership

Main departmental Managers identify main Information assets based on the criteria determining what an information asset is: -

- Primary assets are usually the core processes and information of the activity in the scope.
- Other primary assets such as the organization's processes can also be considered, which will be more appropriate for drawing up an information security policy or a business continuity plan. Depending on the purpose, some studies will not require an exhaustive analysis of all the elements making up the scope. In such cases, the study boundaries can be limited to the key elements of the scope.

Table 1 Threat Codes

Code	THREAT ITEM	example
A	**Alteration**	
B	**Breach**	**Hacking, Virus Attack**
D	**Dissatisfaction**	**Employee, terrorist, Contractors**
I	**Interception**	**Wireless**
N	**Natural Disaster**	**Act of God, Flood,**
O	**Disappearance**	
P	**Power Usurpation**	**Identity Theft**
R	**Revelation [Disclosure]**	
S	**Sabotage**	
T	**Theft & Fraud**	**Internal, Third party, Deception**
U	**Usability [Deprive of Use]**	**Denial of Service, System crash**
X	**Damage**	**Fire,**
Z	**Destruction**	

Table 2 Asset classification

Class letter	Name
D	Data
A	Asset [tangible]
I	ICT equipment
H	Human Resource

Table 3 Assets valuation

Main departmental Managers rate assets against defined criteria for loss of Confidentiality, Integrity and Availability. :-

Confidentiality:

Score	Description
1	Insignificant (i.e. Very Low) - negligible or no damage to asset
2	Minor - Low damage to assets not causing an increase in operational costs
3	Moderate - Some damage or loss causing an increase in operational costs
4	Major - Serious but not complete damage to asset
5	Severe damage to assets - externally visible - considerable damage to business

Integrity:

Score	Description
1	Insignificant (i.e. Very Low) - negligible or no damage to asset
2	Minor - Low damage to assets not causing an increase in operational costs
3	Moderate - Some damage or loss causing an increase in operational costs
4	Major - Serious but not complete damage to assets
5	Severe damage to assets - externally visible - considerable damage to business

Availability:

Score	Description
1	Insignificance can be absorbed and shows no measurable impact - no service disruption
2	Minor - Work distraction; minor increases in support or costs - low disruption to service
3	Moderate - Work delays; noticeable impact on costs and productivity - short disruption to service
4	Major - Work interruption; business commitments delayed with serious costs
5	Catastrophic- Work stoppage and extended service closure; substantial support costs

Overall rating of assets based on highest single rating in any category.

Table 4 Vulnerability/ Probability Identified vulnerabilities to be graded for likelihood and impact using set criteria: -

Rating	Likelihood rating	Explanation
1	Highly unlikely	Greater than 1 in 5 years
2	Unlikely	2 to 5 years
3	yearly	2 in 1 year
4	monthly	2 in 1 month
5	daily	Daily

Table 5 risk rating controls

Rating	insignificant	minor-accepted	moderate-control	major-control	critical-eliminate
Lower limit	1	3	5	13	17
Upper limit	2	4	12	16	26

Risk treatment

Risks will be reviewed and actions agreed with timing and owners assigned. The 'Risk register' will be reviewed by management for updates to risk and a detailed review completed annually. Mitigation factors and monitors will be identified to ensure assumptions made during the risk assessment remain valid.

Review

The Risk assessment and the Risk treatment plan will be reviewed after each Security audit and after each Security incident report to check if ratings for Impact and likelihood need amending.

This methodology will be reviewed and approved by Management at the Security forum meeting and reconfirmed at least annually.

Privacy impact assessments (PIA) (BS10012:2017 6.1.4)

PIAs are sometimes referred to as Data Protection Impact Assessments (DPIAs)

The organization has defined the PIA processes relating to the processing of personal information that:

a) Establish and maintain privacy risk criteria, including:

- Risk acceptance criteria.
- Criteria for performing privacy risk assessments (including where externally mandated); and
- Application of the data protection principles to the data flows to identify privacy risks.

b) Ensure that repeated privacy risk assessment processes are consistent, valid and comparable.
c) Identify the data protection risks associated with the privacy risk assessment process to identify risks associated with:
    - Relevant privacy laws, standards and frameworks.
    - The impact on the rights and freedoms of natural persons.
    - Any physical, material or non-material damage to natural persons; and
    - The impact on the organization (including, but not limited to reputation, regulatory action, financial loss, etc.).
d) Identify high-risk personal information (see 8.2.2.2) and related processes that are high risk.
e) Identify the risk owners.
f) Analyses the privacy risks that:
    - Assess the potential consequences that would result if the risks identified in the privacy risk assessment were to materialise.
    - Assess the realistic likelihood of the occurrence of the risks identified in the privacy risk assessment; and
    - Determines the levels of risk.

g) Evaluate the privacy risks, including:
- Comparison of the results of risk analysis with the risk criteria; and
- Prioritizing the analysed risks for risk treatment.
- The organization retains documented information about the privacy impact and risk assessment process.

NOTE 2 Physical, material or non-material damage means:
- where the processing might give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal information protected by professional secrecy, unauthorized reversal of de-identification, or any other significant economic or social disadvantage.
- Where natural persons might be deprived of their rights and freedoms or prevented from exercising control over their personal information.
- Where special categories of personal information or information relating to criminal convictions and offences or related security measures are processed.
- Where personal aspects are evaluated, such as profiling.
- Where personal information of vulnerable natural persons, of children, is processed; or
- Where processing involves a large amount of personal information and affects many data subjects.

NOTE 3 Vulnerable natural persons are those who, due to their personal circumstances, are especially susceptible to detriment, particularly when a data controller is not acting with appropriate levels of care.
NOTE 4 An example of a risk assessment process (as applied to records) is included in PD1SO/TR 18128:2014 Information and documentation - Risk assessment for records processes and systems.

6.1.5 Privacy risk treatment (BS10012:2017 6.1.5)
The organization defines privacy risk treatment processes to:
a) Select appropriate privacy risk treatment options, considering the risk assessment results.
b) Determine all controls that are necessary to implement the privacy risk treatment option(s) chosen.

NOTE 1 Organizations are required to implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is carried out in accordance with the law, hence they need to design their controls as appropriate, or identify them from any source, including codes of conduct issued by appropriate regulators and supervisory authorities.

- Formulate a privacy risk treatment plan; and
- Obtain risk owners' approval of the privacy risk treatment plan and acceptance of the residual privacy risks.
- The organization shall retain documented information about the privacy risk treatment process.

NOTE 2 the privacy risk assessment and treatment process in this British Standard align with the principles and generic guidelines provided in BS ISO 31000.

NOTE 3 Controls could include, for example, de-identification, pseudonymization, data minimization, reducing the extent and purposes of processing, period of storage, accessibility or technical and organizational information security measures, such as those identified in BS EN1SO/1EC27001.

PRIVACY RISK RATING CHART

Assess each individual risk for the task and enter the score on the Task Risk Assessment sheet. Multiply each score and enter the result in risk rating column. Add together each total to give final risk rating total.

Refer to appendix A & B when completing this risk assessment

Likelihood

SCORE	PROBABILITY OF EXPOSURE	CONTACT WITH HAZARD
0	IMPOSSIBLE	CANNOT HAPPEN
1	ALMOST IMPOSSIBLE	POSSIBLE UNDER EXTREME CONDITIONS
2	HIGHLY UNLIKELY	THOUGH CONCEIVABLE
3	UNLIKELY	COULD HAPPEN
4	POSSIBLE	COULD HAPPEN BUT UNUSUAL
5	EVEN CHANCE	COULD HAPPEN

Consequence

SCORE	IMPACT	PIM DAMAGE LOSS
0	No impact on Personal information	None
1	Personal information disclosed is not sensitive	Company loss of reputation
2	Personal information disclosed could be sensitive	ID theft possible/ Company loss of reputation
3	Personal information disclosed is sensitive	ID theft possible/Company could be subject to claims/ loss of reputation
4	Personal information disclosed a special category see Appendix A	ID theft possible/Company could be subject to claims/ loss of reputation
5	Personal information disclosed is high risk see appendix B	ID theft probable /Company could be subject to claims/ loss of reputation

Action Table

SCORE	ACCEPT RISK/CONSIDERED ACTION
0 –9	MINOR, NO FURTHER ACTION
10 – 19	MEDIUM RISK CONSIDER CONTROLS
20 – PLUS	HIGH RISK CONTROLS REQUIRED

Appendix A special categories (BS10012:2017 6.1.3.2)

When special categories of personal information are being processed, the organization will, in addition, identify, define and document the additional legal basis for the processing of personal information, which shall be selected from one or more of the following:

- Natural person's explicit consent for specific purposes.
- Necessary for employment rights or obligations.
- Necessary for protecting the vital interests of the natural person.
- Necessary for legitimate activities of a foundation, association, or any other non-profit making body

For a political, philosophical, religious or trade union aim, with appropriate safeguards.

- Information deliberately made public by the natural person.
- Necessary for the establishment, exercise or defence of legal claims.
- Necessary for reasons of substantial public interest.
- Necessary for preventive or occupational medicine, assessment of the working capacity of an employee, medical diagnosis, and provision of health or social care systems and services.
- Necessary for reasons of public health or professional secrecy.
- Additional provisions for processing of a kind introduced by national laws regarding the processing of genetic, biometric or health data.

Appendix B High-risk personal information (BS10012:2017.8.2.2.2)

The inventory allows for the explicit identification and documentation of the high- risk categories of personal information processed by the organization.

High-risk categories of personal information can include:

a) Special category personal information.
b) Personal bank account and other financial information.
c) National identifiers, such as national insurance numbers.
d) Personal information relating to vulnerable adults and children.
e) Detailed profiles of natural persons (including children); and
f) Sensitive negotiations which could adversely affect natural persons.