Magma Tech Solution Co., Ltd.

RISK MANAGEMENT
POLICY & FRAMEWORK

Risk Identification • Assessment • Control

Magma Tech Solution Co., Ltd.

MAGMA TECH SOLUTION CO., LTD.

Version 1.0 | Effective 1 January 2026

Document Control	Details
Document Owner	Magma Tech Solution Co., Ltd. – Management
Document Status	Approved by Management
Version	1.0
Effective Date	1 January 2026
Review Frequency	At least annually and following material changes
Approved By	Tapati Bhattacharya – Managing Director

1. Purpose

This Policy & Framework defines how Magma Tech Solution Co., Ltd. identifies, assesses, manages, monitors and escalates risks associated with its business operations and the provision of IT personnel, contractors, secondment, staff augmentation and related workforce services to clients.

The framework is designed to support reliable resource delivery, appropriate handling of information, compliance with applicable obligations, sound administration and timely resolution of service issues.

2. Scope

This framework applies to Management and relevant personnel involved in:

- IT recruitment, candidate sourcing, screening and submission.
- IT outsourcing, secondment, staff augmentation and consultant deployment.
- Consultant onboarding, assignment administration, performance coordination, replacement and offboarding.
- Payroll, invoicing and statutory administration where these services are provided.
- Handling of client information, personal data, credentials, devices and system access where relevant to an assignment.
- Engagement with subcontractors or other third parties where used.

Applicable laws, client contracts, statements of work and client security or operational requirements must be followed. Where requirements differ, the stricter applicable requirement should be escalated for review.

3. Risk Management Principles

- Proportionate: focus on risks relevant to the company's services, scale and client obligations.
- Preventive: identify foreseeable issues early and take reasonable steps to reduce likelihood or impact.
- Accountable: assign an owner to each material risk and mitigation action.
- Documented: maintain appropriate records of risk reviews, decisions, incidents and corrective actions.
- Responsive: escalate significant risks promptly and communicate with the client when required.
- Confidential: protect personal, commercial and client information throughout risk management activities.

4. Roles and Responsibilities

Role	Responsibilities
Management	Approves and oversees this framework; reviews high and critical risks; assigns resources; approves material risk treatment and corrective actions.
Account / Client Coordinator	Monitors service delivery, client feedback, deployment timelines and contract-related issues; escalates material risks.
HR / Recruitment	Manages candidate quality, resource availability, onboarding, replacement coordination, performance feedback and relevant employment records.
Payroll / Finance	Monitors payroll and invoice timelines, payment approvals, reconciliations and applicable statutory administration.
IT / Security Contact, where assigned	Coordinates access, device, confidentiality, data-handling and information-security matters.
Employees / Consultants	Follow company and client requirements, protect information, report concerns promptly and cooperate with investigations or corrective actions.

5. Risk Identification, Assessment and Treatment

Risks are identified through recruitment and deployment planning, client feedback, contract reviews, consultant performance discussions, payroll checks, compliance tracking, security events, complaints, incidents and changes to service or regulatory

requirements. Each material risk is assessed for likelihood and impact, assigned an owner and treated with proportionate actions.

Supplier and subcontractor risks include inadequate capability, service interruption, conflicts of interest, confidentiality failures, unauthorized access to information and non-compliance with applicable legal or contractual requirements. Screening and monitoring should be proportionate to the supplier's role, the criticality of the service and the information or systems to which access is provided.

5.1 Likelihood and Impact Scale

Score	Rating guide
1	Rare / minimal
2	Unlikely / minor
3	Possible / moderate
4	Likely / major
5	Almost certain / severe

Risk Score = Likelihood × Impact. The score supports prioritization; management also considers legal obligations, contract deadlines, client impact, information sensitivity and other relevant circumstances.

Score	Risk Level	Required Response
1–4	Low	Monitor through routine activities.
5–9	Medium	Assign mitigation actions and review progress.
10–16	High	Prioritize mitigation and management oversight.
17–25	Critical	Escalate promptly to Management and take immediate proportionate action.

6. Key Risk Areas and Controls

Risk Area	Control / Response
Resource availability and delayed deployment	Plan sourcing early, monitor required start dates, maintain candidate pipelines where practical and communicate foreseeable delays to the client.
Candidate suitability and skills mismatch	Validate CV details and role-relevant skills; conduct appropriate interviews or checks; retain relevant submission and approval records.
Consultant resignation or unavailability	Use the replacement and escalation process; assess service impact and coordinate next steps with the client in line with contractual arrangements.
Performance and client dissatisfaction	Review client feedback, document concerns, agree improvement actions and escalate unresolved issues.
Contractual and regulatory compliance	Maintain relevant agreements and assignment records; monitor applicable obligations and seek qualified advice where needed.
Visa and work permit matters, where applicable	Track relevant expiry dates and renewal actions; ensure required authorization is in place before deployment.
Payroll, invoicing and payment processing	Use processing calendars, validate inputs, confirm approvals, reconcile amounts and escalate foreseeable delays.
Personal data and confidentiality	Limit access to authorized personnel, use appropriate transfer channels, share only necessary information and follow applicable privacy requirements.
Client systems and information security	Follow client access, acceptable-use and device requirements; remove access at assignment end; report suspected incidents promptly.

Risk Area	Control / Response
Business continuity and key-person dependency	Maintain backup contacts and handover information; identify critical activities and reasonable alternative arrangements.
Fraud, bribery, conflicts and misconduct	Follow the Code of Conduct, raise concerns through appropriate channels and take proportionate corrective action.
Third-party dependency, where applicable	Clarify responsibilities, protect information shared with providers and monitor material service issues.

7. Incident Reporting and Escalation

- Personnel report suspected security or privacy incidents, misconduct, payroll issues, compliance concerns and material service disruptions promptly to their designated Magma Tech Solution Co., Ltd. contact.
- The receiving contact records known facts, immediate actions, potential impact, owner and next steps, while limiting access to sensitive information.
- Management determines whether the client, affected individuals, authorities or other parties must be notified under applicable law or contract.
- Where a client's systems, information or service delivery are affected, the appropriate client representative or designated contact shall be notified in accordance with the applicable contract, agreed procedures and client incident-reporting requirements.
- Corrective actions are tracked to completion, and relevant lessons are incorporated into controls or awareness activities.

  For significant cybersecurity or personal-data incidents, response arrangements should include prompt escalation to Management and the designated IT or service contact, reasonable containment, preservation of relevant evidence, assessment of impact and notification to clients, affected individuals or authorities where required by applicable law or contract.

8. Monitoring and Review

7.1 Business Continuity and Operational Resilience

Management will maintain proportionate arrangements to support critical activities during disruption. These may include backup management and client contacts, access to essential company and client records, alternative payroll processing arrangements, backup personnel for key responsibilities and a process to identify replacement consultants where feasible. Material disruptions must be escalated promptly and affected clients informed in accordance with contractual obligations.

- The Risk Register is reviewed at least quarterly and when a significant incident, service change, client requirement or material risk arises.
- High and Critical risks are reviewed more frequently until actions are completed or residual risk is accepted by authorized Management.
- Risk owners update action status and retain appropriate evidence of completion.
- Management reviews material risks, overdue actions, recurring incidents and lessons learned.
- This Policy is reviewed at least annually, or earlier when services, applicable requirements or client obligations change materially.

9. Risk Acceptance and Corrective Action

Risk treatment may include avoiding, reducing, transferring or accepting a risk. Only authorized Management may accept a material residual risk. A risk that would breach applicable law, required authorization or binding client requirements must not be accepted merely for convenience. Corrective actions should have an owner, target date and completion evidence where appropriate.

10. Records and Document Control

- Maintain the Risk Register, material incident records, review decisions and corrective-action records in an access-controlled company location.
- Retain records for the period required by applicable law, contract and company procedures.

- Share records with clients or other relevant parties only when necessary, duly authorized and consistent with applicable confidentiality, contractual and data-protection obligations.
- Management oversees this Policy and approves material changes.

Appendix A – Risk Register

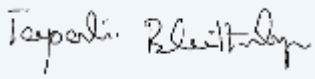
The Risk Register below is a working control record. Ratings and actions should be reviewed as circumstances change. The listed starting scores are management working assessments and should be updated when the actual likelihood, impact or control effectiveness changes.

Risk	L	I	Score	Mitigation / Monitoring	Owner	Status
Delayed consultant deployment	3	4	12 – High	Early sourcing, start-date tracking, client updates	Recruitment / Account	Monitor
Consultant resignation / unavailability	3	4	12 – High	Replacement process and escalation contacts	HR / Account	Monitor
Candidate skills mismatch	2	4	8 – Medium	CV validation and role-based screening	Recruitment	Monitor
Payroll processing delay	2	4	8 – Medium	Payroll calendar, input validation and approval checks	Payroll / Finance	Monitor
Work authorization expiry, if applicable	2	5	10 – High	Expiry tracking and advance renewal follow-up	HR / Administration	Monitor
Unauthorized client data disclosure	2	5	10 – High	Confidentiality, limited access and appropriate transfer channels	Management / IT contact	Monitor
Client-system access not removed at exit	2	5	10 – High	Offboarding checklist and access-removal confirmation	Account / HR	Monitor
Consultant performance concern	3	4	12 – High	Client feedback and documented improvement actions	Account / HR	Monitor
Key contact unavailable	3	3	9 – Medium	Backup contacts and handover notes	Management	Monitor
Contract or statutory obligation missed	2	5	10 – High	Obligation calendar and periodic compliance review	Management / Administration	Monitor

Appendix B – Risk Review Record

Review Item	Record
Review date	24 December 2025 – Management review record
Reviewed by	Tapati Bhattacharya – Managing Director
Material changes since previous review	The Policy establishes the initial risk review baseline. Material changes are assessed during quarterly risk-register reviews and annual policy review.
New or increased risks	New or increased risks are recorded in the Risk Register, assigned an owner and escalated to Management according to their rating.
Overdue mitigation actions	Risk owners record action status and target dates in the Risk Register. Overdue high or critical actions are escalated to Management.
Decisions / escalation required	Management oversees risk treatment and escalation. Risk owners promptly report significant incidents, compliance concerns, consultant deployment issues, data-security incidents or other material risks to Management.
Next review date	By 1 January 2027, and annually thereafter or earlier if material changes occur.

Approval and Acknowledgement

Control	Details
Policy Owner	Magma Tech Solution Co., Ltd. – Management
Approval Status	Approved by Management
Approver	Tapati Bhattacharya – Managing Director
Effective Date	1 January 2026
Next Review	By 1 January 2027, and annually thereafter or earlier if material changes occur.
Management signature	
Date of signature	24th Dec 2025

This Risk Management Policy Framework has been approved by Management and is effective from 1 January 2026.

Risk ratings, assessments and review records shall reflect Magma Tech Solution Co., Ltd.'s actual business position, operations and identified risks. This document represents the Company's internal risk management policies and practices and does not constitute an ISO certification, independent audit report or external assurance.