Supplier Code of Conduct

At Crownpeak Technology Inc. (“Crownpeak”), we value integrity, ethical business practices, and respect for human rights and the environment. We expect our suppliers and business partners to uphold these principles and commit to responsible conduct. This Supplier Code of Conduct outlines our standards and expectations for our suppliers, as well as their affiliated companies, in areas such as labor practices, environmental sustainability, business ethics, and compliance with laws and regulations.

At a minimum, we require that all Suppliers comply with applicable laws and regulations within the geographies where they operate and be open and cooperative with the regulators enforcing such laws. Failure to comply with the Supplier Code during business with Crownpeak will lead to your disqualification as an accepted supplier and will eliminate you from consideration of new business with Crownpeak.

HUMAN RIGHTS

Crownpeak is committed to supporting the protection and advancement of human rights in our business and throughout our supply chain. We expect our suppliers to have appropriate policies and practices in place that apply to their employees and supply chains.

Fair Employment: Suppliers must offer fair wages, benefits, and working conditions to their employees, in line with relevant laws and regulations on working hours, minimum wage, overtime pay, harassment, and workplace safety.

Non-Discrimination: Suppliers must avoid discrimination based on race, color, religion, gender, age, disability, sexual orientation, or any other protected characteristic in their hiring and employment practices.

Forced Labor: Suppliers must not utilize forced labor or involuntary labor, including prison labor or human trafficking, within their operations or supply chain.

Child labor: Suppliers must not hire workers below the legal minimum age for employment according to local and international laws.

BUSINESS ETHICS

Crownpeak is committed to conducting the highest standards of ethical business and expects the same from our suppliers and other business partners. They are fundamental to Crownpeak's core values and play a vital role in building trust, fostering long-term relationships, and contributing positively to society and the environment. Our commitment to ethical business extends beyond mere compliance with laws and regulations; it encompasses a proactive approach to promoting fairness, honesty, respect, and accountability in all business dealings. We expect our suppliers and other business partners to uphold these same values and demonstrate a strong commitment to ethical conduct in all aspects of their operations.

Integrity: Suppliers must conduct their business with honesty, transparency, and integrity, avoiding conflicts of interest, bribery, corruption and unethical practices.

Confidentiality: Suppliers must respect the confidentiality of Crownpeak Technology's information, assets, and intellectual property, ensuring they are protected from unauthorized disclosure or misuse by maintaining appropriate processes.

Privacy: Suppliers must respect individual privacy rights and comply with applicable data protection laws and regulations when handling personal data or sensitive information. In addition, personal data provided by or on behalf of Crownpeak must only be used, accessed, and disclosed as permitted by the Supplier agreement.

Trade and sanctions: Suppliers must adhere to all applicable trade laws, export control regulations, and economic sanctions imposed by relevant authorities in the jurisdictions where they operate or conduct business.

COMPLIANCE AND REPORTING

Crownpeak encourages its suppliers to implement their guidelines for ethical behaviour. Any breach of the obligations contained in this Supplier Code of Conduct will be considered a material breach of contract by the supplier. Crownpeak places a strong emphasis on compliance with laws, regulations, and ethical standards across all aspects of business operations. We expect our suppliers and business partners to align with these compliance requirements and demonstrate a proactive commitment to upholding legal and ethical principles. Not adhering to the standards and expectations outlined in the Code can have serious consequences, potentially leading to contract termination or other remedial actions as deemed appropriate by Crownpeak.

Compliance: Suppliers must follow this Supplier Code of Conduct and any additional contractual requirements specified by Crownpeak Technology. Suppliers must reveal subcontracting agreements and secure written consent from Crownpeak. Subcontractors bring added risk due to potential access to sensitive data or involvement in crucial operations. Furnishing comprehensive details about subcontractors enables the organization to evaluate and address risks linked with external participation, ensuring that subcontractors uphold identical standards and security protocols as the principal supplier.

Monitoring and Evaluation: Crownpeak retains the right to monitor and evaluate supplier compliance with this Code of Conduct through audits, assessments, and other methods.

Business Continuity: Suppliers must develop and maintain a comprehensive business continuity plan that outlines procedures for responding to disruptions such as natural disasters, cyber-attacks, supply chain interruptions, and other emergencies. This plan should include measures for ensuring the continuity of critical operations, communication channels, data protection, and recovery strategies.

Communication: Suppliers must maintain open and transparent communication with Crownpeak regarding any potential risks or disruptions that may impact on their ability to fulfill contractual obligations.

Incident Reporting: Suppliers must promptly report any business continuity incidents or disruptions to Crownpeak and collaborate on recovery efforts as needed.

Reporting Violations: Suppliers should promptly report any breaches of this Code of Conduct or any concerns regarding unethical or illegal behaviour to Crownpeak for investigation and resolution.

ENVIRONMENTAL SUSTAINABILITY

Crownpeak endeavors to manage and leverage our resources in a way that promotes a healthy and sustainable environment. Crownpeak encourages suppliers to implement policies and measures that aim to reduce the environmental impact of their operations.

Compliance: Suppliers must adhere to all applicable environmental laws, regulations and standards in the regions where they operate.

Pollution Prevention: Suppliers must take steps to prevent air, water, and land pollution, including proper waste management and disposal practices.

Conservation of Resources: Suppliers should work towards minimizing their environmental footprint by conserving natural resources, reducing waste, and promoting energy efficiency.

HEALTH AND SAFETY

Suppliers are mandated to prioritize and secure the health, safety, and welfare of their workers and visitors. This responsibility extends to protecting the public from any health and safety risks associated with the suppliers' operations. To achieve this, suppliers must strictly adhere to all relevant laws and regulations applicable to their industry and operational activities. This includes:

Regular Training: Providing ongoing and systematic training programs that equip workers with up-to-date knowledge and skills to perform their duties safely. Training should cover general safety protocols as well as job-specific hazards, including emergency procedures, the proper use of equipment, handling of hazardous materials, and any other relevant safety measures.

Clear Communication: Maintaining open lines of communication where safety information is clearly conveyed and easily accessible. This could include signage, manuals, digital platforms, and regular safety meetings.

Evaluation and Feedback: Implementing processes to regularly evaluate the effectiveness of the training programs and incorporating feedback from workers to continuously improve safety practices.

Safety Culture: Fostering a workplace culture that prioritizes safety, where workers feel responsible for not only their own safety but also the safety of their colleagues and visitors.
By embedding these practices, suppliers can ensure a safer working environment, mitigate risks, and comply with legal standards, thereby promoting the well-being of all individuals associated with their operations.

INFORMATION SECURITY AND DATA PRIVACY

The security of our intellectual property, information and systems is critical to our commercial success. We therefore need our suppliers to respect and safeguard our information by complying with applicable laws and regulations, having appropriate processes and governance in place and working with us to identify and mitigate risks.

Privacy and Data Protection Suppliers must comply with local privacy and data protection laws to respect and protect the privacy and personal data of all individuals relevant to Crownpeak. Suppliers must also comply with the requirements set out in all data processing agreements.

Crownpeak must be notified immediately if anything affects the confidentiality, integrity or availability of personal information (e.g. unlawful destruction, loss, alteration, unauthorized disclosure or access).

Any data incidents or suspected breaches should be reported to Crownpeak within 24 hours. These notifications should be sent to [enter email address] and should be prior to any notification to any government regulator to enable Crownpeak to undertake any remedial work or prepare notifications as may be required by the law.

Intellectual Property Suppliers must safeguard our confidential information, trade secrets and intellectual property (including copyrights, trademarks and patents) from unauthorized access and misuse.

Information Security Suppliers must maintain and apply best practice security to safeguard our data, confidential information, trade secrets and intellectual property, along with the integrity and availability of the products or services being provided. These controls and measures will be subject to regular review as part of Crownpeak's supplier due diligence process. Suppliers must:

Safeguard the security and privacy of their systems and our data throughout their entire supply chain;

Have appropriate technical and organizational measures in place to meet our information security and privacy requirements and standards. These may include:

Appropriate access controls in place to prevent unauthorized access to physical locations, systems, and applications used to process Crownpeak information;

A suite of information security policies and procedures that have been tailored to reflect the security nuances of the supplier's environment and are regularly communicated to all internal stakeholders;

An information security risk management framework (or similar) that facilitates the identification, analysis, evaluation, treatment, and reporting of information security risks;

An information security and data privacy training programme (or similar) that applies to both new hires during induction and existing employees on at least an annual basis thereafter;

Appropriate logging and monitoring controls in place to detect any abnormal or malicious activity on any systems and applications used to process Crownpeak information;

Appropriate incident management processes and controls in place that facilitate the identification, reporting, containment, eradication, and and recovery from information security incidents that may directly or indirectly impact Crownpeak;

Appropriate business continuity and contingency processes and controls in place to ensure that any services provided to Crownpeak can continue to operate, where possible, during any significant business disruptions within the supplier's environment;

Appropriate compliance controls that facilitate the security and protection of any personal data processed by the supplier belonging to Crownpeak;

Appropriate supply chain security controls which apply to the entire lifecycle of a supplier (procurement, onboarding, ongoing monitoring and review, offboarding);

Appropriate software development controls in place to reduce security vulnerabilities within development environments, and to ensure that all code is developed and handled in a secure manner.

The required level of security controls a supplier will need to have in place will depend upon a number of factors, including:

- The type of services provided by the supplier.
- What level of access the supplier has to Crownpeak information.
- The overall level of risk posed by the supplier; and
- The criticality score assigned to the supplier as per our internal processes.

INCIDENT MANAGEMENT

Suppliers must take steps to reduce the risk of an information security incident. Suppliers must ensure that their own information security arrangements and those within their supply chain are appropriate to the requirements of the information assets concerned, and any contractual obligations to Crownpeak. This must include appropriate governance and risk management processes, ensuring access to data is maintained on a need-to-know, least privileged basis and that processes are in place to respond effectively to any incidents. Suppliers should inform us if they become aware of any cyber security incident that could or has compromised our data or services.

Suppliers must cooperate fully with us in any investigation, conduct root cause analysis and follow up actions where required.

ARTIFICIAL INTELLIGENCE (AI)

Where AI forms any part of the services suppliers are delivering to Crownpeak, we expect suppliers to be transparent about this and tell us at the earliest opportunity. AI must not be introduced into live services without our prior written consent. Should any AI related problems arise, we expect to be told promptly.

We expect suppliers to use AI responsibly and within the law. Suppliers should ensure their use of AI avoids any unlawful discrimination or bias and adheres to all data privacy and equality law obligations and aligns to relevant standards and guidance. This includes those issued by the UK's National Cyber Security Centre (NCSC) and the European Telecommunication Standards Institute (ETSI).

Suppliers must not use Crownpeak data as input data or use it to train an AI solution without our prior written consent. Any AI usage must respect Crownpeak's Intellectual Property rights.

COMMITMENT TO IMPROVEMENT

Crownpeak encourages ongoing enhancement of supplier practices related to labor, ethics, and the environment. We value open communication and collaboration with our suppliers to tackle challenges, implement best practices, and promote responsible business conduct throughout our supply chain. By adhering to this Supplier Code of Conduct, suppliers demonstrate their dedication to shared values of integrity, responsibility, and sustainability, making a positive impact on the communities and environments where we operate.