Supplier Information Security and Cyber Hygiene

As a world leading zoological institution, we believe that our suppliers play an important role in our endeavour to protect wildlife. We are strongly committed to a safe digital environment and the safeguarding of our guest data, and this commitment extends to our suppliers and the procurement of goods and services.

We value suppliers who are transparent, ethical, and environmentally and socially responsible.

We expect our suppliers to adhere to the standards as set out in this **Supplier Information Security and Cyber Hygiene** standards and to ensure that Suppliers, their employees, sub-contractors, their service providers and other third parties that our suppliers work with are aware of and understand these standards.

1 Definition

1.1 **Information security** is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information. It also involves actions intended to reduce the adverse impacts of such incidents. Protected information may take any form, e.g. electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge). Information security's primary focus is the balanced protection of the confidentiality, integrity, and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity.

1.2 **Cyber hygiene** is a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted.

2 Supplier obligation and commitment

2.1 Supplier shall comply to all relevant Acts, Regulations and Code of Practice of Singapore including any amendments or re-enactment thereto, such as Personal Data Protection Act (PDPA), Computer Misuse Act and Cybersecurity Act.

2.2 Supplier shall provide assurance to us that they will do their upmost to protect our interest through their information security and cyber hygiene practices. Supplier can provide assurance, where possible thru the submission of their information security policies and standards, certification, declaration, or equivalent commitment in a letter.

2.3 Supplier shall submit "Information Security Assessment Questionnaire" when requested for our assessment of their commitment in protecting us interests and acknowledge that submission may be used in the consideration of contract award. Supplier agrees to provide only accurate, truthful information in their submission. All submission will be kept confidential.

2.4 Supplier shall provide a named Data Protection Officer (DPO), per PDPA to us.

2.5 Supplier shall be fully responsible for the conduct of their staff, their sub-contractors and the sub-contractor's staff (collective known as Supplier Staff).

2.5.1 Supplier Staff shall be responsible for taking reasonable care and use of the our assets, not limited to computing devices, docking station, display monitor, keyboards, mouse, presentation pointers, cables, physical storage media issued to and put under Supplier Staff's care; including keeping them under lock and key. In the event of misused, damaged and/or lost due to negligence, the Supplier agrees to solely bear the cost of replacement.

2.5.2 Supplier Staff shall abide by our access controls/rules regardless of if the access controls/rules are automated through system authentication or otherwise. Supplier Staff shall not circumvent any security software and measures.

2.5.3 Supplier Staff shall comply to the our prevailing policies and standards and shall protect the our data, as appropriate, and use it only for valid business and/or work purposes.

2.6 Supplier shall promptly report to the us on any Supplier Staff misconduct, ill intent, and any cybersecurity events, theft, loss or unauthorised disclosure of the proprietary information.

3 Contract Terms and Conditions

3.1 Supplier will need to agree to the following terms and conditions:

"7.1. The Supplier shall, prior to the execution of this Agreement, submit copies of and/or provide website links to the Supplier's information security policy and standards, or similar policy, or a written commitment to protect the Client's information, data and software, or any similar evidence in respect thereof (for each of the foregoing, whether in tangible or intangible form) and hardware (collectively, "**Data**") from any cyber threat, attack, damage, ransom, theft or loss, or similar. The Supplier shall also submit an information security assessment questionnaire (the "**Information Security Assessment Questionnaire**") for the purposes of providing the Client with the necessary assurances, and enabling the Client to conduct its due diligence assessment of the Supplier and ascertain the Supplier's commitment to protecting the Data. The Supplier represents and warrants that all information submitted to the Client in connection with the foregoing is true, accurate, current and complete.

"7.2 In the event that the Client deems that the Supplier's protection of the Client's Data based on the submissions described in Clause 7.1 are unsatisfactory or inadequate for the purposes of the Supplier's provision of the Scope under this Agreement, as determined by the Client in its sole and absolute discretion, the Client shall provide written notice to the Supplier of such deficiencies (which notice shall be deemed conclusive for the purposes of the assessment of the deficiencies), and the Supplier shall exercise best efforts at all times and render all necessary cooperation to the Client to implement remedial measures in respect of such deficiencies, as soon as practicable and at no cost to the Client, and in any event, within 90 calendar days of the Supplier's receipt of such written notice. At any time upon the Client's written request, the Supplier shall, within 45 calendar days from the date of the Client's written request, provide adequate supporting written verification of the implementation of the relevant remedial measures, and/or engage at the Supplier's own cost an independent and reputable third party audit firm to carry out an independent audit and provide written findings and certification as to the adequacy of such remedial measures, in each instance, the sufficiency of which may be determined by the Client in its sole and absolute discretion. The Client may immediately terminate the Agreement by written notice to the Supplier in the event that the Supplier fails to do any of the foregoing in this Clause 7.2."

"7.3 Supplier acknowledges that any direct or indirect event that compromises or may compromise the confidentiality, integrity, security and/or availability of any information system, and/or any unauthorised storage and/or transmission of the Client's data to any unauthorised external destination(s), device(s) or recipient(s), as determined in the Client's sole and absolute discretion

("**Cybersecurity Incident**"), may result in damage to the Client, including but not limited to reputational, financial and operational losses. In the event of a Cybersecurity Incident that arises from, is caused by, and/or occurs in connection with, Supplier's act(s) or omission(s), Supplier shall be liable to and indemnify Client in accordance with Clause 10 of the GTCs, for all damages, losses, costs, charges, penalties, and expenses, arising from any mitigation measures undertaken in response to the Cybersecurity Incident, as determined in the Client's sole and absolute discretion. Supplier shall provide all necessary co-operation and take such steps as Client may deem necessary and expedient in furtherance of the recovery from the Cybersecurity Incident."

"7.4 With reference to Clause 20.2 of the GTCs, in the event that the Client consents to the Supplier sub-contracting any part of the works or services to be performed by the Supplier, the Supplier shall ensure that its arrangements with its sub-contractors contain terms that are similar to but no less favourable to the Client in respect of Clauses 7.1 to 7.3 above."