Information Security Addendum

Silverchair has established and agrees to maintain a written information security and privacy program (the "***Information Security Program***") designed to comply with this Information Security Addendum and applicable law. Terms not defined herein have the meaning set forth in the DPA.

As part of its program, Silverchair has implemented and agrees to maintain administrative, technical, and physical security safeguards designed to protect the confidentiality, integrity, and availability of Personal Data, including but not limited to:

- **Administrative and Organizational Safeguards**
    - Silverchair maintains policies and procedures for the security of Personal Data, including the following:
        - Written information security policies that set forth Silverchair's procedures with regard to maintaining the safeguards set forth in this Information Security Addendum.
        - Incident Response Plan, which sets forth Silverchair's procedures to investigate, mitigate, remediate, and otherwise respond to security incidents.
    - Silverchair conducts assessments of the risks and vulnerabilities to the confidentiality and security of Personal Data.
    - Silverchair monitors the effectiveness of its Information Security Program, and will evaluate its Information Security Program and information security safeguards in light of any material changes to its operations or business arrangements.
    - Silverchair maintains role-based access restrictions for its systems, including restricting access to only those Silverchair employees that require access to perform the Silverchair Services or to facilitate the performance of such Silverchair Services, such as system administrators, consistent with the concepts of least privilege, need-to-know, and separation of duties.
    - Silverchair periodically reviews its access lists to ensure that access privileges have been appropriately provisioned and regularly reviews and terminates access privileges for Silverchair employees that no longer need such access.
    - Silverchair assigns unique usernames to authorized Silverchair employees and requires that Silverchair employees' passwords satisfy minimum length and complexity requirements and be changed periodically.
    - Silverchair provides training to employees, as relevant for their roles, on confidentiality and security.
    - Silverchair requires employees to acknowledge Silverchair's Information Security Program.
    - Silverchair has a policy in place to address violations of its Information Security Program.
- **Technical Security**
    - Silverchair logs system activity—including authentication events, changes in authorization and access controls, and other system activities.
    - Silverchair maintains network security measures, including but not limited to firewalls, to segregate its internal networks from the internet, risk-based network segmentation, and anti-virus and malware protection software.
    - Silverchair has implemented workstation protection policies for its systems, including automatic logoff after a period of inactivity and locking the system after a defined number of incorrect authentication attempts.
    - Silverchair requires multi-factor authentication on its systems for administrative users.

- Silverchair conducts periodic vulnerability scans on all systems storing, processing, or transmitting Personal Data to identify potential vulnerabilities and risks to Personal Data.

- Silverchair remediates identified vulnerabilities in a risk-prioritized and timely manner, including timely implementation of all high-risk mitigating manufacturer- and developer-recommended security updates and patches to systems and software storing, transmitting, or otherwise Processing Personal Data.

- **Physical Security**

  - Silverchair restricts access to its facilities, equipment, and devices to Silverchair employees with authorized access on a need-to-know basis.

  - Silverchair tracks the location of its equipment, devices, and electronic media and maintains a record of such locations.