APPENDIX - Information Security Requirements

This Information Security Requirements Appendix ("Appendix") is incorporated into [the Frame Agreement for Services] (the "Agreement") dated [insert date] executed between Sanoma Corporation ("Sanoma") and [insert name] ("Supplier"), together the "Parties".

1. SCOPE

1.1 Subject to the terms and conditions of the Agreement, all services performed by Supplier under the Agreement ("Services") shall comply with the policies, standards, and requirements set forth in this Appendix, **as applicable in the context of the Services**. This Appendix sets out the Supplier's key responsibilities concerning the security requirements for the IT environments, facilities, and personnel used to create, develop, and manage the Services.

1.2 This Appendix and the requirements set forth herein are in addition to, and not in lieu of, other requirements incorporated into the Agreement. The requirements of this Appendix apply to the Supplier as well as its subcontractors, and the Supplier shall be fully liable for the performance of its subcontractors.

2. GENERAL SECURITY REQUIREMENTS

2.1 Supplier shall at all times comply with the security requirements set forth in this Appendix.

2.2 Supplier shall provide Services which are designed, delivered, and at all times support compliance with industry standards and best practices, such as ISO 27001/27002, ISF Standard of Good Practices for Information Security and ISO 22301 for Business Continuity Management Systems, whenever feasible and not in conflict with other agreed requirements. If credit card data is processed, Payment Card Industry Data Security Standard must be complied with.

2.3 Supplier shall independently and proactively follow industry developments and endeavor to incorporate the newest approved best practices into its day to day operations. Within fourteen (14) calendar days of Sanoma's request, Supplier shall provide Sanoma its policies and methodologies for following and incorporating changes in industry best practices.

3. SECURITY MANAGEMENT

3.1 Security responsibilities within the Supplier's organization shall be assigned by senior management to nominated individuals. The responsibilities shall include (but are not limited to) overall security, risk management, privacy, and controls for handling Personal Data (as defined by the applicable legislation and the Data Protection Appendix). The nominated individuals shall be notified to Sanoma. The Supplier shall have a documented process for reviewing the implementation of security within its organization.

3.2 Monitoring and evaluation of security and privacy related topics regarding the Services shall be covered as part of regular service meetings or by a separate working group with representatives of each Party ("Security Governance").

3.3 Supplier shall establish and maintain a security architecture which provides a framework for the standard security controls throughout the Supplier's organization.

3.4 Supplier shall have a comprehensive, documented information security policy and related guidelines, and communicate them to all individuals with access to the Supplier's relevant information and systems. The information security policy shall be approved by Supplier's senior management.

3.5 Supplier shall adopt and document security measures for information systems and the creation, use, modification, and deletion of data. The measures shall be commensurate to the data contained and processed in the systems, and be based on an information classification scheme (e.g. company confidential, confidential and secret). Information ownership must be defined at all times.

3.6 Supplier shall implement and regularly update a security risk management system, which incorporates emerging threats, possible business impacts, and probabilities of occurrence. Supplier shall modify security related processes, procedures, and guidelines accordingly.

3.7 Supplier shall comply with EU as well as other applicable statutory, regulatory, and legal obligations relating to the Services provided to Sanoma, and its systems used to provide such Services or containing Sanoma related data.

3.8 Supplier shall maintain system documentation in adequate level until the end of the Service lifecycle. At the termination of the Services for any reason and in addition to any obligations set out in the Agreement, the Supplier shall: (1) hand over the system documentation to Sanoma, assuming the system is owned by Sanoma, (2) provide Sanoma assistance in transferring the Services to Sanoma or another service provider, (3) return to Sanoma any Sanoma related data in a jointly agreed format, and (4) wipe the data and/or destroy any Sanoma related data from its systems.

4 AUDIT RIGHTS

4.1 Supplier shall detail how Sanoma related data is protected to ensure that Sanoma data security, privacy and other compliance requirements are met.

4.2 On a regular basis Supplier shall conduct independent reviews and assessments (e.g. internal/external audits, certifications, vulnerability and penetration testing) on the Supplier's compliance with this Appendix. Visibility of the assessment results shall be provided to Sanoma, including at the minimum the scope of the assessment, security findings and their mitigation status. Supplier shall immediately report any critical vulnerabilities or findings to Sanoma (Service Representatives and cert@sanoma.com).

4.3 Sanoma (or an independent Third Party appointed by Sanoma) may conduct an audit of the Supplier according to an audit plan upon twelve (12) calendar days' prior written notice. Sanoma may also request to audit Supplier's subcontractors respectively. Additionally, Sanoma or its designated security auditing partners may perform ad hoc testing and application security reviews of any service that is about to be deployed or that is currently operated by Supplier. Sanoma strives to inform the Supplier five (5) calendar days in advance of such testing and reviews.

4.4 Sanoma is responsible for the costs of the reviews and tests referred to in section 4.3. However, should the testing or review reveal any violation or breach of this Appendix by Supplier, Supplier shall without delay compensate Sanoma for the costs arising from the audit and remedy the breach.

4.5 If the audits, reviews or assessments reveal any violation or breach of this Appendix by the Supplier, the Supplier shall without delay remedy the breach without any cost to Sanoma.

4.6 All policies, guidelines, plans, systems, schema, and methodologies set forth in this Appendix shall be submitted to Sanoma within twelve(12) calendar days at any time as requested by Sanoma. Additionally, Supplier shall provide visibility to Sanoma related security incidents, security incident investigations and authority requests as part of Security Governance.

4.7 Supplier shall provide Sanoma visibility on where Sanoma related data is processed, stored, transmitted, and where it may be accessed from. Supplier shall inform Sanoma in writing in advance should the Supplier intend to transfer Sanoma related data to another location and obtain Sanoma's prior written consent for such transfer (cert@sanoma.com).

5. INCIDENT HANDLING & RESPONSE

5.1 Supplier shall have adequate and documented issue/incident response procedures (or plans) and nominated persons to timely react and prevent any further damage caused by security, privacy or any other compliance issues, vulnerabilities, or incidents.

5.2 Supplier shall inform Sanoma without delay in case of any Sanoma related security incident (cert@sanoma.com).

5.3 Supplier shall at all times maintain the capability to prevent, monitor, detect, investigate, and respond to security and privacy incidents.

5.4 Supplier shall have proper forensic procedures in place to ensure chain of custody, which is required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident.

5.5 Supplier shall maintain capability to detect potentially suspicious network behaviors and/or file integrity anomalies, and capability to support forensic investigative capabilities in the event of a security breach.

6. BUSINESS CONTINUITY

6.1 Supplier shall have business continuity / disaster recovery plans documented and implemented. To minimize the impact of a realized risk event (e.g. natural disasters, accidents, equipment failures, or sabotage) on the organization, including subcontractors providing end-to-end service to Supplier's customers ("Disaster Recovery and Business Continuity Plan"). Supplier shall demonstrate the functioning of such plans by conducting regular tests and exercises. At Sanoma's request, Supplier shall provide reports on the tests and exercises it has undertaken to verify its ability to recover from a realized risk event.

6.2 Supplier shall also facilitate the recovery of information assets through a combination of preventive and recovery controls. Said controls shall be in accordance with applicable statutory, regulatory and legal requirements and consistent with industry standards and best practices. The availability requirements (such as recovery times, recovery points, levels of recovery & resumption etc.) for Disaster Recovery and Business Continuity Plan must be agreed with Sanoma.

6.3 Supplier shall enforce a documented backup policy that ensures the capability to fulfill agreed Service Levels and continuity requirements during emergency situations. The backups shall be stored in secure storage. Actual restoration of the backups must be tested regularly to ensure their usability. Supplier shall store backups of Sanoma related data based on the criticality of the data. At a minimum, Supplier shall store daily backups for the last thirty (30) calendar days and monthly backups for the last twelve (12) months, unless required otherwise by statutory, regulatory, or legal obligations. Additionally, Supplier shall store system backups for the last twelve (12) months to ensure recovery from a clean version in case of contamination of the whole service.

7. PERSONNEL SECURITY AND AWARENESS

7.1 Supplier shall ensure that its employees and subcontractors are bound by statutory or contractual confidentiality obligations prior to accessing Sanoma related data. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.

7.2 Supplier shall perform proper vetting (including background and other security checks) for critical staff according to relevant national legislation at no additional cost to Sanoma.

7.3 Supplier shall maintain an appropriate entry and exit procedure for personnel changes that includes disabling user access rights upon termination of employment with the Supplier or termination of assignment for Sanoma.

7.4 Supplier shall conduct security and privacy awareness training (or refresher sessions) during induction and at least annually for all existing employees and new hires performing Services for Sanoma. Due emphasis shall be given to client confidentiality, understanding the agreed confidentiality obligations and specifically the sensitivity of personal data. Advanced security training shall be given to key roles (e.g. administrators or employees with full access to Sanoma related data) working with sensitive information and assets (e.g. consumer data, financial data or employee data).

7.5 Supplier shall have documented guidelines to define acceptable usage for e-mail, instant messaging, internet access, VOIP, wireless access, social media, and any other electronic communications. Supplier

shall ensure that all employees have at all times access to up-to-date guidelines, and Supplier shall have measures in place to maintain and increase awareness of the guidelines.

8. PHYSICAL SECURITY

These physical security requirements apply only to data centers assuming Sanoma related data is fully encrypted in the premises where it is processed and it is not extracted (e.g. laptops fully encrypted, data never printed).

8.1 Adequate physical security perimeters (e.g. fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) shall be implemented to safeguard sensitive data and information systems.

8.2 Supplier shall have a premises access control system, where in:

- Every individual shall have a unique access card and/or key to access the premises
- Physical access control log data shall be stored for at least ninety (90) calendar days unless otherwise restricted by local legislation
- Access to sensitive areas (e.g. server rooms) shall be granted separately by named owners of the area and only for those who need access to the area to perform their work related duties.
- There shall be a regular access rights auditing and revocation process.

8.3 Supplier shall have up-to-date documented policies and/or guidelines for responding to premises intrusions and a capability to timely respond to intrusions to premises where Sanoma assets or related data is processed, transmitted or stored.

8.4 ID-badges shall show easily identifiable differentiation between employee classifications (e.g. internals, externals, visitors).

8.5 Supplier shall have a documented visitor policy and all visitors must be identified, registered, logged, and accompanied by an employee from Supplier at all times.

8.6 Cleaning and maintenance work shall be closely supervised in sensitive areas and performed during office hours. Keys, access codes, and intrusion alarm revocation codes to areas where Sanoma related data is processed, transmitted or stored shall not be given to anyone without a valid business need, including cleaning and maintenance staff.

8.7 Supplier or their respective sub-contractor hosting servers containing Sanoma related data shall have adequate fire protection in server rooms.

8.8 Supplier shall install and maintain continuously recording video cameras (CCTV) of appropriate quality for facial recognition and used to passively monitor individual physical access to sensitive areas (including entrances & exits), where Sanoma related data is stored, processed or transmitted.

8.9 Supplier shall ensure that all power and telecommunications equipment, cabling carrying data or supporting information services are protected from interception or damage and designed with redundancies, alternative power source and alternative routing.

8.10 If Sanoma related data is printed and/or stored in paper form, Supplier shall use secure/dedicated printers, shredders, and locked bins for hardcopy information when appropriate according to information sensitivity. Supplier shall also have a clean desk practice.

9. IT SECURITY

9.1 Supplier must implement information security measures to protect Sanoma related data against unauthorized or accidental access, use, disclosure, deletion, loss, alteration or amendment. Sanoma related data shall only be stored and processed in an environment where security and privacy controls have been implemented.

9.2 Supplier shall logically isolate all Sanoma related data from its own, and all of its other customers' data so that Sanoma related data is processed, transmitted, accessed, and stored by a minimum number of authorized persons who only have access to such data that they need to perform their work related duties (role-based access control). This concerns also backups and logs.

9.3 Identity and Access Management for development and administrative purposes must fulfill the following requirements, including but not limited to:

- Supplier shall have policies and/or guidelines for approving, creating, and terminating user access rights
- Supplier shall have policies and/or guidelines for strength and rotation of access credentials, e.g.
    a. Implementing an automatic and forced password resetting process
    b. Prohibiting and preventing the use of default or weak passwords
    c. Securely handling and delivering credentials (such as user name and password)
- Every user must be individually identifiable. Common/shared user accounts are prohibited and the use of them shall be prevented.
- Any credentials must have the minimum permissions required for their intended use.
- As part of software development two-factor authentication shall be implemented based on threat analysis. In case of administrative remote access to environment with Sanoma related data two-factor authentication is always required.

9.4 Supplier shall ensure that there is a sufficient audit trail of the use of access privileges (changes, who, what, when) in place for Sanoma related data. Logs regarding user access and all activity that creates, changes, or deletes Sanoma related data shall be collected and stored for at least twelve (12) months or more, if required by statutory, regulatory or legal obligations. Access to log data shall be restricted to prevent compromise and misuse of log data. Sanoma shall have right to know who has access to its data. Supplier shall support Sanoma in case of security investigations or requests from authorities by providing visibility to relevant logs.

9.5 Supplier shall protect at Supplier's own premises and/or systems all Sanoma data by appropriate controls including, but not limited to network segmentation using host based firewall or network based firewall, firewall log monitoring, network intrusion detection or prevention systems (IDS/IPS), web application firewalls, log management, correlation capability, malware prevention for servers and end-user computing devices, application and infrastructure vulnerability scanning. Supplier shall maintain documented processes to ensure that all network devices are protected from unauthorized access and that all updates are conducted based on an agreed maintenance plan.

9.6 Supplier shall deploy any host systems using a standardized secured configuration (hardened, i.e. provide only necessary ports, protocols and services to meet the functionality requirements). Sufficient vulnerability and patch management processes shall be maintained and followed in order to implement security patches and fixes in a timely fashion according to industry best practices and the level of criticality.

9.7 Sharing of Sanoma related data shall only be undertaken through secure data sharing portals or tools. The use of insecure file transfer protocols is strictly forbidden.

9.8 Supplier shall maintain TLS certificates needed to provide the Services, and monitor the expiry of all TLS certificates, and manage their timely replacement.

9.9 Supplier shall encrypt all information and/or data by using current industry-standard strong encryption, key management and related standards (e.g. AES-256 / SHA-256 or NIST latest recommendations), when processing, transmitting and/or storing personal data, consumer data, Sanoma confidential or secret information in public cloud environments, including consumer cloud storage services, and transmission of data over the public Internet.

9.10 When transferring e-mail over the public Internet, the preferred way is to use end-to-end or gateway-to-gateway encryption (e.g. TLS). At minimum the Supplier shall have the capability to send adequately encrypted attachments (e.g. AES-256 / SHA-256 or NIST latest recommendations).

9.11 Supplier shall establish policies and procedures and implement mechanisms for effective key management to support encryption of data in storage and in transmission as well as authentication. Key management and key usage shall be separated duties.

9.12 Supplier shall have remote access and remote work policies, practices, guidelines and restrictions in place. Wireless access and remote connections shall be protected from eavesdropping (e.g. VPN).

9.13 If Sanoma's virtual meeting solution is not used, Supplier shall ensure that the following controls are implemented for the virtual meeting solution:

- Remote control of the web camera is disabled
- The web camera shall automatically shut down when a virtual meeting session has ended

9.14 All laptop hard disks and other client devices (like USB-memory sticks, netbooks, smartphones, tablet computers, portable media players etc.) and other removable/back up media containing Sanoma related data shall use full data encryption.

9.15 Supplier shall securely and permanently destroy/wipe Sanoma related data in a Sanoma-approved manner from all media and/or devices when it is no longer required for the Services. Any old or broken media containing Sanoma related data shall be effectively and permanently wiped without possibility to retrieve any data or destroyed prior to being decommissioned or reused. Supplier shall ensure that necessary backup arrangements are taken into account prior disposal.

9.16 Workstations and other end-user devices that are used to access Sanoma related data shall be installed from standardized installation images or by using standardized installation or configuration procedures. Devices shall be configured to be resistant to attacks in accordance with industry standards and best practices and the means of connecting to networks, IT services or other end-user devices shall be designed to be secure, and protected against unauthorized disclosure or alteration of business information. All software used in workstations shall be regularly patched and personal firewalls shall be in use.

9.17 All and any device used or added to the end user environment (e.g. Bring your own device - BYOD) shall be approved, protected by appropriate security controls and supported by standard operating procedures or instructions for acceptable use.

9.18 Automated, up-to-date and functional malicious code protection (such as an antivirus and anti-spyware/malware) shall be installed in all systems used to deliver end-to-end service for Sanoma.

9.19 Operational systems and software must be subject to strict change management control. Change management procedures (including changes to security features) shall be agreed in the Security Governance.

9.20 Supplier must not process production data in non-production environments, unless relevant security and privacy controls as set forth in this Appendix have been implemented to the non-production environment.

9.21 Administrative tools capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.

10. SECURITY AND PRIVACY BY DESIGN

10.1 IT system development activities must be conducted in accordance with a documented system development methodology, which includes the requirement for information security measures at each stage of the system development lifecycle.

10.2 Supplier shall design and implement all its products and Services delivered to Sanoma properly taking into account relevant privacy and security related requirements (e.g. privacy and security by design). This means in practice that for any new or changed functionality Supplier shall conduct:

- architectural/design threat analysis and for identified risks define which controls are to be implemented and which risks will be treated in some other jointly agreed way.

- security and privacy assessment (e.g. internal/external audits or testing) for features that have been flagged as a risky area in threat analysis, or are a part of a security or privacy control.

Architectural/design threat analysis should be based on data flow diagrams and cover at the minimum but not limited to:

- Identity and access management
- Impacted user experience/business logic flows
- Impacted personal data flows
- Software dependencies (e.g. third party components, libraries)
- Deployment architecture
- Software development pipeline
- Auditability (e.g. logging)
- Service/Product lifecycle until retirement

10.3 Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g. OWASP Top 10 for Web Applications and OWASP ASVS for testing coverage) and adhere to applicable legal, statutory, or regulatory compliance obligations.

10.4 On Sanoma's request Supplier shall provide visibility of the identified risks, threats and assessment results.

10.5 Supplier shall include security controls such as: (1) secure coding standards/guidelines, (2) change controlled configuration (3) third party components vetting and vulnerability management (4) security tests that establishes that each of the security requirements has been met, (5) apply, test, and validate the appropriate patches and updates and/or workarounds, (6) ensure that all security issues shall be evaluated and fixed based on risk analysis.