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

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 Services.

This Appendix and the requirements set forth herein are in addition to, and not in lieu of, other requirements incorporated into the Agreement.

1.1 General Security requirements

Supplier shall at all times comply with the Sanoma security policies, guidelines and standards as set forth in this Appendix.

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 and Disaster Recovery, whenever feasible and not in conflict with other agreed requirements. Where credit card data is processed Payment Card Industry Data Security Standard must be complied with.

Supplier shall independently and proactively follow industry developments and endeavor to incorporate the newest approved best practices in to 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.

1.2 Audit Right

Audit rights are agreed in Data Protection Appendix. In addition at Sanoma's request Supplier shall provide a written report on all locations where Sanoma's data assets are processed, transmitted, stored, or accessed from to ensure compliance with requirements set by Sanoma, external authorities, and/or regulations.

All policies, guidelines, plans, systems, schema, and methodologies set forth in this Appendix shall be submitted to Sanoma within 14 working days at any time as requested by Sanoma.

2. SECURITY MANAGEMENT

2.1 Control over security and privacy shall be provided by a high-level working group or committee ("Security Governance") and shall be supported by a nominated senior executive of the Supplier. The Security Governance shall consist of representatives of each Party and shall hold periodic meetings to monitor and evaluate security related topics.

2.2 Supplier's senior management shall assign security responsibilities to nominated individuals and shall have a written process to review the implementation of security within its organization. Supplier's senior management shall nominate an individual responsible for the overall security, risk management, information privacy, and controls for handling Personal Data (as defined by the applicable legislation and the Data Protection Appendix). The nominated individual shall be notified to Sanoma.

2.3 Supplier shall produce 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. Information security policy shall be approved by Supplier's senior management.

2.4 The Supplier shall have its own information classification schema based on information sensitivity (for example, company confidential, confidential, and secret) and information ownership must be defined at all times.

2.5 Supplier shall document appropriate controls and interpretation on how information is to be created, used, and destroyed. These controls must be commensurate to the value of the information asset. In case Sanoma defines the information classified as secret, necessary controls shall be agreed separately with the Supplier.

2.6 Supplier shall implement the use of secure/dedicated printers, shredders, and locked bins for hardcopy information when appropriate according to information sensitivity. Supplier shall also have a clean desk practice.

2.7 Supplier shall establish a process for classifying information systems and adapt security measures commensurate to the systems' criticality. Visibility to Sanoma shall be provided through security measures including at the minimum, but not limited to, security findings and fixed status follow up, security incident follow-up, security incident investigation and authority request follow-up.

2.8 Supplier shall implement and regularly update 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.

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

2.10 Supplier shall comply with the 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.

2.11 Security performance metrics and security reporting requirements will be agreed in the Security Governance.

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

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

2.14 Independent reviews and assessments (e.g., internal/external audits, certifications, vulnerability and penetration testing) shall be performed as agreed by the Security Governance. The assessment shall be performed at least annually, or at regular intervals as agreed in the Security Governance. The Supplier shall share the results of the assessment in the Security Governance.

2.15 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) handover the system documentation to 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.

3. INCIDENT HANDLING & RESPONSE

3.1 The 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.

3.2 Supplier and its subcontractors shall immediately notify and escalate to Sanoma any such event, which may have any impact on Sanoma, using commonly predefined and agreed communication channels and agree with Sanoma all necessary steps for incident management.

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

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

3.5 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.

3.6 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.

4. EMERGENCY RESPONSE

4.1 The Supplier shall create and maintain a documented and implemented emergency response plan, focusing primarily on the safety of people (including externals, visitors, and guests), premises, and assets. The plan shall be based on risk assessment and aim at mitigating imminent risks that are termed as "accepted" or "tolerated" during the risk management process (“Emergency Response Plan”).

4.2 Periodic testing on the Emergency Response Plan, such as planned evacuations and rescue drills, etc. shall be conducted and the result of such exercises duly recorded.

4.3 Supplier shall include into the Emergency Response Plan and take all necessary steps to prevent and detect emergency situations by means of fire and smoke alarm systems; sprinklers, fire-fighting equipment etc. in compliance with relevant national legislation.

4.4 Supplier shall train emergency response teams (“ERT”) on emergency response routines on a continuous periodic basis.

4.5 Supplier shall communicate and make available emergency guidelines to all employees and visitors to sites and periodically reinforce such guidelines by means of communication, awareness campaigns, or participation in planned exercises and drills.

5. BUSINESS CONTINUITY

5.1 Supplier shall have business continuity / disaster recovery plans documented and implemented, specifically for the Sanoma engagement and the Sanoma related data.

5.2 Supplier shall maintain business continuity and disaster recovery plans, to minimize the impact of a realized risk event (e.g. natural disasters, accidents, equipment failures, and sabotage) on the organization (“Disaster Recovery and Business Continuity Plan” as further specified in the Agreement). Supplier shall also facilitate recovery of information assets through a combination of preventive and recovery controls. Said controls shall be in accordance with applicable legal requirements and consistent with industry standards. The availability requirements as applicable (such as recovery times, recovery points, levels of recovery & resumption etc.) for Disaster Recovery and Business Continuity Plan must be agreed with Sanoma.

5.3 Supplier shall conduct tests and exercises on its Disaster Recovery and Business Continuity Plan in order to validate the business continuity arrangements and availability requirements as requested by Sanoma. Supplier shall demonstrate the functioning of such plans to Sanoma by providing reports on the technical testing it has undertaken to verify its ability to recover from a disaster and continue to meet its continuous service performance and availability targets.

5.4 Supplier shall enforce data backups and store them in a secured storage that ensures the capability to fulfill agreed Service Levels and continuity requirements during emergency situations. These backups must be based on a documented backup cycle/policy and must be tested regularly by actual restoration to ensure their usability. Supplier shall store Sanoma related data for a minimum of the last ninety (90) days, or more if required by Sanoma or by statutory, regulatory, or legal obligations.

5.5 Supplier shall create and maintain a plan for joint business continuity testing, including subcontractors providing end-to-end service to Sanoma, to ensure acceptable levels of continuity and recovery of the Service provided to Sanoma. Such a plan shall include, without limitation, details on the type of testing that is included, as well as the times and intervals of such testing. Supplier undertakes to arrange such joint testing not less than once per calendar year. If a joint test would show evidence of material shortcomings in Supplier's supply chain, Supplier shall take all necessary action to remedy the situation and arrange further joint testing session within thirty (30) calendar days of the previous test.

5.6 Supplier shall have asset inventory, which includes all information necessary in order to recover from a disaster, including type of asset, format, location, backup information and license information.

6. PERSONNEL SECURITY

6.1 Supplier shall ensure that its personnel and subcontractors comply with the confidentiality obligations as defined in this Agreement, and have agreed on confidentiality prior to accessing Sanoma's data.

6.2 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.

6.3 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.

6.4 A formal disciplinary or sanction policy shall be established for employees and subcontractors who have violated security policies and procedures. 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. AWARENESS AND COMPETENCE DEVELOPMENT

7.1 Supplier shall conduct security and privacy awareness training (or refresher sessions) during induction at least annually for all existing employees and new hires performing Services for Sanoma. Due emphasis shall be given to the handling of client confidentiality, understanding the agreed confidentiality obligation and specifically un-launched product information, social media guidelines (and restrictions), as well as sensitivity of any third party data contained on Sanoma systems. Advanced security training shall be given to key roles working with sensitive information and assets (e.g. consumer data, financial data, employee data, health data).

8. PHYSICAL SECURITY

If Sanoma related data is fully encrypted in the premises (e.g. office building) where it is processed, then these physical security requirements apply only to the data centers.

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) 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 create and maintain a documented policy and have a capability to timely respond to premises intrusions where Sanoma assets or specific 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's information 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 information shall have adequate fire protection in server rooms, such as Inergen automatic fire extinguishing system.

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. Records shall be stored for at least 90 days, unless otherwise restricted by local legislation.

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.

9. HANDLING OF SANOMA INFORMATION

9.1 Supplier shall document and implement processes for protecting the confidentiality of Sanoma's product and technology information.

9.2 Sharing of data (e.g. personal data or other Sanoma confidential information) shall only be undertaken through the Sanoma approved data sharing portals or tools. The use of insecure file transfer protocols is strictly forbidden.

10. IT SECURITY

10.1 Supplier must implement information security measures to protect Sanoma's 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.

10.2 Supplier shall isolate all Sanoma Information from its own and all of its other customers' information 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 backup and log information.

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

- Supplier shall have policies for approving, creating, and terminating user access rights
- Supplier shall have policy for strength and rotation of access credentials, e.g.
    a. Implement an automatic and forced password resetting process

    b. Prohibiting and preventing the use of default 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 implement two-factor authentication based on threat analysis. In case of administrative remote access to environment with Sanoma related data two-factor authentication is always required.

10.4 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 needs to be restricted to prevent compromise and misuse of log data. Sanoma shall have right to know who has access to its data. Audit trail has to be maintained and provided to Sanoma on request.

10.5 Supplier shall protect at Supplier's own premises and/or systems all Sanoma data by appropriate controls including, but not limited to host intrusion detection and prevention, host network firewall, malware prevention for servers and end-user computing devices, application and infrastructure vulnerability and configuration compliance scanning.

10.6 Supplier shall deploy any host systems using a standardized secured configuration (hardened, i.e. provide only necessary ports, protocols and services to meet Sanoma's needs). 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.

10.7 Supplier shall properly maintain the TLS certificates needed to run the Service so that new valid TLS certificates are installed before old ones expire. Supplier shall monitor the expiry of all TLS certificates, and initiate and manage the timely replacement of expiring TLS certificates.

10.8 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 a capability to send adequately encrypted attachments (e.g. AES-256 / SHA-256 or NIST latest recommendations) shall exist.

10.9 Supplier shall have a documented electronic communications policy 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 to the policy, and Supplier shall have measures in place to maintain and increase awareness of the policy.

10.10 Supplier remote access and remote work policies, practices, guidelines and restrictions shall be included in the information security policies of the Supplier. Wireless access or remote connection shall be protected from eavesdropping (e.g. VPN).

10.11 Supplier may not use web cameras for virtual meetings unless the following controls have been implemented:

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

10.12 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. Wireless access or remote connection shall be protected from eavesdropping (e.g. VPN).

10.13 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 confidential Sanoma information or customer information shall use full data encryption.

10.14 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.

10.15 Any Supplier used or provided end-user device shall be configured to be resistant to attacks 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. This includes that all software used in workstation is regularly patched. Supplier shall securely and permanently destroy/wipe Sanoma information in a Sanoma-approved manner from all media/devices when it is no longer required for use in relation to Sanoma.

10.16 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.

10.17 Supplier shall maintain at Supplier own premises and/or systems effective documented processes to ensure that all network devices are prevented from unauthorized access and all updates are conducted based on agreed maintenance plan. Supplier shall protect all hosts by appropriate controls including, but not limited to firewall log monitoring, network intrusion detection/prevention system (IDS/IPS), web application firewalls, log management, and correlation capability.

10.18 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.

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

10.20 Supplier shall conduct security review for new or changed functionality and features that have been flagged as a risky area in threat analysis, or are a part of a security control.

10.21 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.

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

10.23 Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.

10.24 Policies and procedures shall be established and mechanisms implemented 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.

10.25 Workstations that are used to access Sanoma related data shall be installed from standardized installation images or there should be standard installation procedures in place and securely configured in accordance with industry and security best practices. Personal firewall shall be installed in all workstations. Any other devices used to process or handle Sanoma related data, shall be approved prior adding it to end user environment, protected by appropriate security controls and supported by standard operating procedures or instructions for acceptable use.

10.26 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.

11. SOFTWARE DEVELOPMENT SECURITY

11.1 Supplier shall design and implement all its products and Services delivered to Sanoma properly taking into account relevant privacy, internet safety 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

11.2 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.

11.3 Supplier shall bring continuous visibility to Sanoma of the identified risks, threats and assessment results.

11.4 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) days in advance of such testing and reviews. Supplier shall immediately report any Critical Vulnerabilities (as defined below) or findings to Sanoma. Sanoma is responsible for the costs of the reviews and tests Sanoma or its designated security auditing partners conduct at Sanoma's initiative 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.

Critical Vulnerability means a vulnerability scored as, or equivalent in severity to, a CVSS (Common Vulnerabilities and Scoring System, latest applicable version) base and/or temporal scores equal to or higher than 7.0.

11.5 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) information on 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 all security issues shall be evaluated and fixed based on risk analysis.

11.6 Identity and Access Management for services developed or provided for Sanoma must implement the needs identified through architectural review/threat analysis

- Following Sanoma policies for approving, creating, and terminating user access rights
- Following Sanoma policy for Credentials Management
- Every user shall have a unique user ID. 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