Appendix 3 – Security Measures Description

This Security Measures Description ("SMD") sets out the standards of the security measures agreed herein, by Wolters Kluwer Danmark A/S("Wolters Kluwer") and Customer ("Customer"). Each of Wolters Kluwer and Customer are referred to as a "Party" and together the "Parties".

1. Scope of SMD

1.1 Customer has entered into an Agreement with Wolters Kluwer regarding provision of Service(s). This Service Measures Description ("SMD") shall apply for the following Service(s).

- Capego SmartSign
- Capego SmartFlow
- Capego Teamwork Plus
- Capego Teamwork Standard
- Finsit

1.2 The Service(s) listed in section 1.1 are within this SMD referred to as "SMD Service(s)".
1.3 This SMD sets out the security measures that Wolters Kluwer shall maintain in connection to providing the SMD Service(s) to Customer.
1.4 The SMD Service(s) are hosted by Microsoft (Azure) in Europe unless otherwise stated.

2. Information security policy

2.1 Policies and guidelines – Wolters Kluwer has implemented a Global IT Security Policy that encompasses a variety of policies for managing information and technology assets intended to protect underlying applications and data. Wolters Kluwer has also implemented an Application Security Policy which defines Wolters Kluwer requirements for the secure development, testing, deployment and monitoring of software applications. Associated with the policies Wolters Kluwer has implemented a set of detailed internal guidelines and procedures.
2.2 Information Security Risk Assessment – On an annual basis, Wolters Kluwer conducts an audit and information security risk assessment of our security strategy, technical capabilities and performance with respect to the SMD Service(s).
2.3 Human Resources –Wolters Kluwer reviews, and updates as needed, its personnel policies relevant to information security.

3. IT Security

3.1 The following areas are covered in the Wolters Kluwer Global IT Security Policy:
- Information Technology Security Management and Organization
- Risk Assessment

- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Operations Security
- Communication Security
- Third-Party Service Providers
- Encryption
- Access Control
- Information System Life Cycle Management
- Information Technology Security Incident Management
- Business Continuity Management
- Compliance

The policy is being further detailed in a number of guidelines and procedures.

4. Application software security

4.1 The following areas are covered in the Wolters Kluwer Application Security Policy:

- Application Security Standard
- Secure Usage of 3rd Party Software
- Secure Usage of Open Source Software
- Secure Usage of External Software Services
- Application Security Training
- Application Security Scanning
- Vulnerability Remediation
- Exception Requests
- Reviews of Security Policy

The policy is being further detailed in a number of guidelines and procedures.

5. Human resources

5.1 Background Checks – Wolters Kluwer executes background checks during the hiring process for all full time employees.
5.2 Acceptable Use Policy – Wolters Kluwer has an Acceptable Use Policy (AUP) for its employees, temporary staff and contractors defining acceptable use and access to Wolters Kluwer and its affiliates' information systems.
5.3 Security Awareness Training – Wolters Kluwer has an information security awareness training program for its employees including at least annual security training for all employees.

6. Infrastructure from Microsoft Azure

6.1 The SMD Service(s) are run on infrastructure provided by Microsoft Azure. The Azure data centers comply with industry standards such as ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2014, ISO/IEC 20000-1:2011, ISO/IEC 22301:2012, ISO/IEC 9001:2015 and NIST SP 800-53 for security and reliability and are managed, monitored and administered by Microsoft Operations staff.
6.2 A detailed documentation of security measures in Azure can be found in the Microsoft Azure documentation on https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data.
6.3 If, in the future, different cloud providers are used in lieu of, or in parallel to, Microsoft Azure, such providers will be required to meet the same level of industry and security standards.

7. SMD Service(s) infrastructure credentials

7.1 Provisioning – All credentials used in conjunction with the infrastructure, operating systems, or databases supporting the SMD Service(s) are supported by an identity management request-based system that requires applicable management approval for access and privilege changes.
7.2 Termination – All SMD Service(s) credentials are to be disabled within 24 hours of an employee's termination date.
7.3 Passwords – Wolters Kluwer has a minimum standard password policy for access to SMD Service(s) and databases. Password complexity and the changing of password at regular intervals is enforced and all passwords must meet the criteria enforced at each time.
7.4 Lockout – Accounts will be locked after repeated consecutive invalid login attempts. Thereafter, accounts can only be unlocked by the applicable data center Service Desk, or once the lockout timer has expired.
7.5 All administrative access to hosting environments are protected using multifactor authentication (MFA).

8. Role separation

8.1 Wolters Kluwer define and document the roles and responsibilities for the employees of Wolters Kluwer and its Service Providers who support infrastructure and services for the SMD Service(s). Each such person/function will be given the amount of privilege necessary in order for such person/function to fulfil the duties of the role he or she is currently assigned.
8.2 Application Credentials for SMD Service(s) Customers - Application credentials are managed by Customer. Customer's administrator account can create, delete and modify application User IDs (UID), and can delegate account control to one or more UID account(s) associated with that Customer's application account. The application UIDs are only valid when used with the SMD Service(s).
8.3 The system leverages the provided cloud support to maintain strict access to information based on user role.

9. Incident response and management

9.1 The Incident policy ensures there is a written incident response plan as well as defined phases of incident handling/management.
9.2 Job titles and duties for handling computer and network incidents are limited to specific individuals and tracking and documentation is ensured throughout the incident through to resolution.
9.3 Management personnel are designated, as well as backups, who will support the incident handling process by acting in key decision-making roles.
9.4 Organization-wide processes are implemented for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, including the mechanisms for such reporting, and definition of necessary information in such incident notification.
9.5 Contact information for relevant third-partes in the event of a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners are documented and kept up to date.
9.6 All employees are informed of the process for reporting computer anomalies and incidents to the incident handling team.
9.7 Response exercise and test scenarios for incident management is conducted for the workforce involved to maintain awareness and comfort in responding to real-world threats.

10. Environment separation

10.1 Environments – Wolters Kluwer has logical environment separation for the SMD Service(s) as described below in this section. Depending on the service involved there may also be physical separation.
10.2 Corporate – Wolters Kluwer has a corporate network supporting general employee and internal business activities. This network is physically and logically separated from networks supporting hosted applications such as in the SMD Service(s).
10.3 Development and Test – Wolters Kluwer has development and testing environments that are separate from stage and production environments.
10.4 Production – Wolters Kluwer has dedicated environments for the SMD Service(s). The production environments are separated from the corporate, development, and test environments.

11. Data recovery

11.1 Backup – Customer data is being backed up using AES-256 based encryption and will be kept and can be restored within 365 days in case of data corruption. The restoration of data within the backup period is provided as a separate service. Backups of assignments (compliance data within a product specific domain, like closing of books or tax) are handled in an application specific manner.
11.2 Retention – Customer data that is not deleted by Customer will be part of backups for as long as Customer has an active service. Data that has been backed up and is deleted by Customer will be maintained as part of backups for 30 days from the time of deletion. If a customer terminates the SMD Service(s) the data will be kept in backups for a period of maximum 60 days from the termination of the service.

12. Availability and disaster recovery

12.1 Redundancy – Wolters Kluwer deploys all computing components for SMD Service(s) such that several instances are running in parallel in the same data centre. In addition, data storage is replicated over two sites meaning that there are multiple copies of all user data.

12.2 High Availability Environments – Wolters Kluwer maintains, for the SMD Service(s) a highly available environment configuration. Using existing and standard public cloud services several instances are running at the same time. Failover between these instances is done in an automated way and outside the direct involvement of Wolters Kluwer.

12.3 Disaster Recovery (DR) – The Service has DR capabilities. In the unlikely event of the primary site being unreachable, Service operations is moved to a secondary site. The recovery time objective (RTO) is 24 hours and the recovery point objective (RPO) is one hour.

12.4 Health Monitoring – Wolters Kluwer maintains automated health monitoring of all computing systems supporting the SMD Service(s). The monitoring system is intended to automatically generate alerts when monitoring thresholds have been exceeded.

12.5 Performance Monitoring – Wolters Kluwer maintains automated performance monitoring of all computing systems supporting the SMD Service(s). The monitoring system is intended to automatically generate alerts when monitoring thresholds have been exceeded.

12.6 Performance Testing – Wolters Kluwer maintains a formal performance and scalability testing process. All major code changes undergo formal performance testing before being deployed to the production environment.

12.7 Capacity Planning – Wolters Kluwer maintains a capacity planning process to assess whether the appropriate amount of computing assets will be available in the production environment to support all Customers.

13. Operations management

13.1 Release Management – Wolters Kluwer maintains a release management and code promotion process for the SMD Service(s). This process is intended to ensure code is tested in a controlled environment, which mimics the production environment, using realistic test cases. Code will be promoted from the testing environment to the staging environment to allow for IT automation and source image validation before being promoted to production.

13.2 Change Management – Wolters Kluwer maintains a change management process. All changes to infrastructure hosting SMD Service(s) will be detailed in a change request, be scheduled in predetermined change window, and require applicable management approval.

13.3 Incident Management – Wolters Kluwer, with its applicable Service Providers, maintains an incident management process. The incident management process is intended to facilitate the resolution of, provide for a root cause analysis for, and ensure remediation steps are completed for any service disruption to the SMD Service(s).

13.4 Security Management – Wolters Kluwer, with its applicable Service Providers, maintains a security incident management process. This process defines steps for minimizing loss of data, preserving evidence, escalation of support to a specialized information technology forensics team, vulnerability identification, vulnerability remediation, and notification guidelines.

13.5 Key Performance Indicators – Wolters Kluwer tracks application uptime, service disruptions, the root cause of material disruptions, and the implementation of any remediation.

14. Additional security measures

14.1 Antivirus and Malware – Wolters Kluwer uses antivirus and malware protection software designed to protect computing equipment hosting the SMD Service(s) and end users.

14.2 Network Intrusion Detection System (NIDS) – Wolters Kluwer maintains Network Intrusion Detection Systems designed to provide certain protections for all environments.

14.3 Network Intrusion Prevention System (NIPS) – Wolters Kluwer maintains Network Intrusion prevention Systems designed to provide certain protections for all environments.

14.4 Security Information and Event Management (SIEM) – Wolters Kluwer maintains SIEM monitoring technology in any production environment.

14.5 SIEM events will be monitored by the security operations center (SOC) team with set thresholds for event escalation.

14.6 Vulnerability Scans – Wolters Kluwer regularly conducts internal and external vulnerability scans. The results are not made available to Customers.

14.7 Penetration Testing – Wolters Kluwer regularly commission a third party external penetration test. An executive summary of results may be made available to Customers upon request and subject to confidentiality requirements.

14.8 Data in transit and at rest is encrypted according to industry best practices.

15. Security logs

15.1 Routers, Switches, Firewalls, and Load Balancers – Allow changes to router configuration to be tracked.

15.2 Servers – Allows users login events to be tracked as individual messages.

15.3 Security and Event Log Management – Wolters Kluwer maintains security and event logs for a minimum of thirty days.

15.4 Routers, Switches, Firewalls, and Load Balancers - Allows configured system events such as memory utilization, CPU utilization, rule utilization, network errors, packet loss, and other messages designed to provide administrators with information regarding the health and performance of the device to be captured.