Appendix D-1 to Aproove Saas Contract : Security and solution hosting provider specs.

The hosting company retained by Aproove is Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052 USA.

Microsoft Ireland Operations Limited (Carmenhall Road, Sandyford, Dublin 18, Ireland) is the official corporate representative of Microsoft concerning Data Protection for European and Swiss operations.

The hosting solution informations can be downloaded from :

- http://azure.microsoft.com/fr-fr/support/trust-center/
- http://go.microsoft.com/fwlink/?linkid=392408&clcid=0x40c

As from October 2014 :

Design and Operational Security

Microsoft has developed industry-leading best practices in the design and management of online services, including:

- **Security Centers of Excellence.** The Microsoft Digital Crimes Unit, Microsoft Cybercrime Center, and Microsoft Malware Protection Center provide insight into evolving global security threats.
- **Security Development Lifecycle (SDL).** Since 2004, all Microsoft products and services have been designed and built from the ground up using its Security Development Lifecycle - a comprehensive approach for writing more secure, reliable and privacy-enhanced code.
- **Operational Security Assurance (OSA).** The Microsoft OSA program provides an operational security baseline across all major cloud services, helping ensure key risks are consistently mitigated.
- **Assume Breach.** Specialized teams of Microsoft security engineers use pioneering security practices and operate with an 'assume breach' mindset to identify potential vulnerabilities and proactively eliminate threats before they become risks to customers.
- **Incident Response.** Microsoft operates a global 24x7 event and incident response team to help mitigate threats from attacks and malicious activity.
- Security Controls and Capabilities

Azure delivers a trusted foundation on which customers can design, build and manage their own secure cloud applications and infrastructure.

- **24 hour monitored physical security.** Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.
- **Monitoring and logging.** Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by

devices within the environment and providing timely alerts. In addition, multiple levels of monitoring, logging, and reporting are available to provide visibility to customers.

- **Patching.** Integrated deployment systems manage the distribution and installation of security patches. Customers can apply similar patch management processes for Virtual Machines deployed in Azure.
- **Antivirus/Antimalware protection.** Microsoft Antimalware is built-in to Cloud Services and can be enabled for Virtual Machines to help identify and remove viruses, spyware and other malicious software and provide real time protection. Customers can also run antimalware solutions from partners on their Virtual Machines.
- **Intrusion detection and DDoS.** Intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of Azure.
- **Zero standing privileges.** Access to customer data by Microsoft operations and support personnel is denied by default. When granted, access is carefully managed and logged. Data center access to the systems that store customer data is strictly controlled via lock box processes.
- **Isolation.** Azure uses network isolation to prevent unwanted communications between deployments, and access controls block unauthorized users. Virtual Machines do not receive inbound traffic from the Internet unless customers configure them to do so.
- **Azure Virtual Networks.** Customers can choose to assign multiple deployments to an isolated Virtual Network and allow those deployments to communicate with each other through private IP addresses.
- **Encrypted communications.** Built-in SSL and TLS cryptography enables customers to encrypt communications within and between deployments, from Azure to on-premises datacenters, and from Azure to administrators and users.
- **Private connection.** Customers can use ExpressRoute to establish a private connection to Azure datacenters, keeping their traffic off the Internet.
- **Data encryption.** Azure offers a wide range of encryption capabilities up to AES-256, giving customers the flexibility to implement the methods that best meets their needs.
- **Identity and access.** Azure Active Directory enables customers to manage access to Azure, Office 365 and a world of other cloud apps. Multi-Factor Authentication and access monitoring offer enhanced security.

Penetration Testing

Microsoft conducts regular penetration testing to improve Azure security controls and processes. We understand that security assessment is also an important part of our customers' application development and deployment. Therefore, we have established a policy for customers to carry out authorized penetration testing on their applications hosted in Azure. Because such testing can be indistinguishable from a real attack, it is critical that customers conduct penetration testing only after obtaining approval in advance from Azure Customer Support. Penetration testing must be conducted in accordance with our terms and conditions. Requests for penetration testing should be submitted with a minimum of 7-day advanced notice.

Independently verified

By providing customers with compliant, independently verified cloud services, Microsoft makes it easier for customers to achieve compliance for the infrastructure and applications they run in Azure. Microsoft provides Azure customers with detailed information about our security and compliance programs, including audit reports and compliance packages, to help customers assess our services against their own legal and regulatory requirements.

Azure is committed to annual certification against ISO/IEC 27001/27002:2013, a broad international information security standard. The ISO/IEC 27001/27002:2013 certificate validates that Microsoft has implemented the internationally recognized information security controls defined in this standard, including guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

The audit included the Information Security Management System (ISMS) for Azure, encompassing infrastructure, development, operations, management, support, and in-scope services. The certificate issued by the British Standards Institution (BSI) is publically available.

Additionally, Microsoft Azure services have incorporated the controls that embody ISO/IEC 27018 – an extension of the ISO 27001 standard with a code of practice governing the processing of personal information by cloud service providers. ISO 27018 provides controls that reflect considerations specifically for protecting personally identifiable information in public cloud services. For example, the ISO 27018 controls prohibit the use of customer data for advertising and marketing purposes without the customer’s express consent. ISO 27018 also provides clear guidance for cloud service providers for the return, transfer and/or secure disposal of personal information of customers leaving their service and requires the cloud service provider to identify any sub-processor before customers enter into a contract, and inform customers promptly of new sub-processors, to give customers an opportunity to object or terminate their agreement.

SOC 1/SSAE 16/ISAE 3402 and SOC 2 Attestations

Azure has been audited against the Service Organization Control (SOC) reporting framework for both SOC 1 Type 2 and SOC 2 Type 2. Both reports are available to customers to meet a wide range of US and international auditing requirements.

The SOC 1 Type 2 audit report attests to the design and operating effectiveness of Azure controls. The SOC 2 Type 2 audit included a further examination of Azure controls related to security,

availability, and confidentiality. Azure is audited annually to ensure that security controls are maintained.

Audits are conducted in accordance with the Statement on Standards for Attestation Engagements (SSAE) No. 16 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402 put forth by the International Auditing and Assurance Standards Board (IAASB). In addition, the SOC 2 Type 2 audit included an examination of the Cloud Controls Matrix (CCM) from the Cloud Security Alliance (CSA).

The audit included the Information Security Management System (ISMS) for Azure, encompassing infrastructure, development, operations, management, support, and in-scope services. Customers should contact Azure Support (or new customers can contact their account representative) to request a copy of the SOC 1 Type 2 and SOC 2 Type 2 reports for Azure.

Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is designed to provide fundamental security principles to guide cloud vendors and to assist prospective customers in assessing the overall security risk of a cloud provider. Detailed information about how Azure fulfills the security, privacy, compliance, and risk management requirements defined in the CCM version 1.2 is also published in the CSA's Security Trust and Assurance Registry (STAR). In addition, the Microsoft Approach to Cloud Transparency paper provides an overview of how Microsoft addresses various risk, governance, and information security frameworks and standards, including the CSA CCM v1.2.

Federal Risk and Authorization Management Program (FedRAMP)

Azure has been granted a Provisional Authority to Operate (P-ATO) from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) at a Moderate impact level based upon the FIPS 199 classification. Following a rigorous security review, the JAB approved a provisional authorization that an executive department or agency can leverage to issue a security authorization and an accompanying Authority to Operate (ATO). This will allow U.S. federal, state, and local governments to more rapidly realize the benefits of the cloud using Azure.

FedRAMP is a mandatory U.S. government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services.

The FedRAMP audit included the Information Security Management System (ISMS) for Azure, encompassing infrastructure, development, operations, management, support, and in-scope services. Government agencies can request the Azure FedRAMP security package. Microsoft intends to pursue FedRAMP certification for Azure Government.

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act of 2002 was implemented to provide agencies the ability to document and implement information security programs within their operational systems.

Previously, cloud providers were required to undergo FISMA assessments by individual federal agencies. Azure received an ATO from the General Services Administration under FISMA. In 2011, the FedRAMP program was created and designed to streamline the process for cloud service providers

and agencies and has replaced FISMA authorizations as the preferred approach to validating the security of cloud services.

The FISMA audit included the Information Security Management System (ISMS) for Azure, encompassing infrastructure, development, operations, management, support, and in-scope services. Government agencies can request the current Azure FedRAMP security package.

Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS)

Microsoft has reviewed the Azure Government policies and procedures to verify that it meets the requirements necessary for U.S. state and local agencies to use in-scope services to store and process Criminal Justice Information. Azure will contractually commit and sign the FBI CJIS security addendum, which commits Azure to the same requirements that law enforcement and public safety must meet. Azure continues to work with a variety of states to enter into additional CJIS Information Agreements, which provide additional information to law enforcement authorities about the nature of the services, and ensure appropriate background screening for operating personnel.

Payment Card Industry (PCI) Data Security Standards (DSS) Level 1

Azure is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standards (DSS) as verified by an independent Qualified Security Assessor (QSA), allowing merchants to establish a secure cardholder environment and to achieve their own certification.

The PCI DSS is an information security standard designed to prevent fraud through increased controls around credit card data. PCI certification is required for all organizations that store, process or transmit payment cardholder data. Customers can reduce the complexity of their PCI DSS certification by using compliant Azure services.

The audit included the Information Security Management System (ISMS) for Azure, encompassing infrastructure, development, operations, management, support, and in-scope services. The Azure PCI Attestation of Compliance and Azure Customer PCI Guide are available for immediate download.

United Kingdom G-Cloud OFFICIAL Accreditation

Azure has received OFFICIAL accreditation from the UK Government Pan Government Accreditor. Azure is available on the G-cloud Framework and details can be found on the UK's Digital Marketplace.

The OFFICIAL rating benefits a broad range of UK Public Sector organizations, including Local and Regional Government, National Health Service (NHS) trusts and some central government bodies who hold or transact public sector data for business conducted at the OFFICIAL level of Security Classification. Details of the OFFICIAL accreditation can be found here and form part of the UK Government's Cloud Security Principles.

OFFICIAL accreditation covers the Azure in-scope services listed on the Azure Trust Center.

Australian Government Information Security Registered Assessors Program (IRAP)

Azure has been assessed against the Australian Government Information Security Registered Assessors Program (IRAP) and a letter of compliance has been issued for in-scope services. The IRAP assessment provides assurance for public sector customers (and the partners that serve them) that

Microsoft has appropriate and effective security controls in place for the processing, storage and transmission of Unclassified Sensitive data within Microsoft Azure. Unclassified Sensitive data represents the majority of federal government, healthcare, education and state government data in Australia.

Multi-Tier Cloud Security Standard for Singapore (MTCS SS 584:2013)

Azure has achieved Level-1 certification with the Multi-Tier Cloud Security Standard for Singapore (MTCS SS), a cloud security standard, developed under the Singapore Information Technology Standards Committee (ITSC) to provide businesses with greater clarity on the levels of security offered by different cloud service providers. The standard covers areas such as data retention, data sovereignty, data portability, liability, availability, business continuity, disaster recovery, and incident management.

A rigorous assessment was conducted by the MTCS Certifying Body and included Microsoft development, operations, support, and in-scope services.

HIPAA Business Associate Agreement (BAA)

HIPAA and the HITECH Act are United States laws that apply to healthcare entities with access to patient information (called Protected Health Information, or PHI). In many circumstances, for a covered healthcare company to use a cloud service like Azure, the service provider must agree in a written agreement to adhere to certain security and privacy provisions set forth in HIPAA and the HITECH Act. To help customers comply with HIPAA and the HITECH Act, Microsoft offers a BAA to customers as a contract addendum.

Microsoft currently offers the BAA to customers who have a Volume Licensing / Enterprise Agreement (EA), or an Azure only EA enrollment in place with Microsoft for in-scope services. The Azure only EA does not depend on seat size, rather on an annual monetary commitment to Azure that allows a customer to obtain a discount over pay as you go pricing.

Prior to signing the BAA, customers should read the Azure HIPAA Implementation Guidance. This document was developed to assist customers who are interested in HIPAA and the HITECH Act to understand the relevant capabilities of Azure. The intended audience includes privacy officers, security officers, compliance officers, and others in customer organizations responsible for HIPAA and HITECH Act implementation and compliance. The document covers some of the best practices for building HIPAA compliant applications, and details Azure provisions for handling security breaches. While Azure includes features to help enable customer's privacy and security compliance, customers are responsible for ensuring their particular use of Azure complies with HIPAA, the HITECH Act, and other applicable laws and regulations, and should consult with their own legal counsel.

EU Model Clauses

Microsoft offers customers E.U. Standard Contractual Clauses that provide additional contractual guarantees around transfers of personal data for in-scope services. Microsoft’s implementation of the E.U. model clauses has been validated by European Union data protection authorities as being in line with the rigorous privacy standards that regulate international data transfers by companies operating in its member states. Microsoft is the first company to receive joint approval from the

E.U.'s Article 29 Working Party for its strong contractual commitments to comply with E.U. privacy laws no matter where data is located.

Food and Drug Administration 21 CFR Part 11

The Food and Drug Administration Part 11 of Title 21 Code of Federal Regulations, Electronic Records; Electronic Signatures (21 CFR Part 11) applies to entities that maintain records or submit information to include records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in FDA regulations. Part 11 also applies to electronic records submitted to the Agency under the Federal Food, Drug, and Cosmetic Act (the Act) and the Public Health Service Act (the PHS Act).

Since Part 11 became effective in 1997, the Food and Drug Administration has publicly emphasized their intent and commitment to overcome unnecessary restrictions on the use of electronic technology, significant costs of compliance and barriers to innovation and technology advances that stand in the way of public health benefit. The Part 11 requirements for validation, audit trails, record retention, record copying, and legacy systems and others introduce potential barriers and restrictions especially for agencies working in constrained time, resource or emergent public health crisis.

Azure's deep partnership with customers and partners in public sector health and life sciences industry resulted in the Qualification Guideline for Microsoft Azure. Working with the Qualification Guideline, entities are able to demonstrate Azure services and execution fulfills Part 11 requirements. To learn more about the customers and partners who have qualified their regulated applications running on Azure, download the Guide or the recorded webinar "Qualifying Microsoft Azure for Regulated Applications in the Life Sciences" from Montrium.

The Azure platform components which are within scope of this review include: Cloud Services (Web, Worker and VM roles), Azure Storage (Blobs, Queues, and Tables), Networking (Traffic Manager, Virtual Network), and Virtual Machines.

Family Educational Rights and Privacy Act (FERPA)

FERPA is a Federal law that protects the privacy of student education records, and imposes requirements on U.S. educational organizations regarding the use and disclosure of student education records. Educational organizations can use Azure to process data, such as student education records, in compliance with FERPA. Microsoft agrees to use and disclosure restrictions imposed by FERPA, will only use Customer Data to provide organizations with the Azure service, and will not scan Customer Data for advertising purposes.

Federal Information Processing Standard (FIPS)

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. The National Institutes of Standards and Technology (NIST) publishes the list of vendors with validated FIPS 140-1 and 140-2 cryptographic modules. Azure uses Microsoft cryptographic modules in the validated list published by NIST, enabling customers to configure and use Azure Virtual Network services in a way that helps meet their information encryption requirements.

Trusted Cloud Service Certification developed by China Cloud Computing Promotion and Policy Forum (CCCPPF)

Azure operated by 21Vianet is among the first batch of Cloud Services Providers in China to pass the Trusted Cloud Service Certification developed by China Cloud Computing Promotion and Policy Forum (CCCPPF) by providing an open platform, high-quality Service Level Agreement (SLA), powerful data recovery capabilities and robust customer benefits.

As part of the trusted cloud service certification result, Azure operated by 21Vianet's Virtual Machines, Cloud Storage and SQL Database were tested and evaluated within the SLA framework in terms of 16 indexes including data management, service quality, and rights protection. The test results issued by the CCCPPF are publically available.

Multi-Level Protection Scheme (MLPS)

Multi-Level Protection Scheme is based on the Chinese state standard (GB/T 22239-2008) and issued by the Ministry of Public Security. The certification labels target systems from level 1 to 5 (with 5 being the highest) based on their risk profiles. The MLPS provides assurance for both the management and technical security of the target system.

Data Protection and data security

Privacy is one of the foundations of Microsoft's Trustworthy Computing. Microsoft has a longstanding commitment to privacy, which is an integral part of our product and service lifecycle. We work to be transparent in our privacy practices, offer customers meaningful privacy choices, and manage responsibly the data we store.

The Microsoft Privacy Principles, our specific privacy statements, and our internal privacy standards guide how we collect, use, and protect Customer Data. General information about cloud privacy is available from the Microsoft Privacy Web site.

The Azure Privacy Statement describes the specific privacy policy and practices that govern customers' use of Azure.

Location of Customer Data

Microsoft currently operates Azure in data centers around the world. In this section, we address common customer inquiries about access and location of Customer Data.

Customers may specify the geographic area(s) ("geos" and "regions") of the Microsoft datacenters in which Customer Data will be stored. Available geos and regions are shown below

MAJOR REGION	SUB-REGION
United States	East US (Virginia) East US 2 (Virginia) Central US (Iowa) West US (California) North Central US (Illinois) South Central US (Texas)
Europe	North Europe (Ireland) West Europe (Netherlands)
Asia Pacific	Southeast Asia (Singapore) East Asia (Hong Kong)
Japan	Japan East (Saitama Prefecture) Japan West (Osaka Prefecture)

Brazil	Brazil South (Sao Paulo State) One-way replication to US South Central (Texas)
Australia	Australia East (New South Wales) Australia Southeast (Victoria)

Microsoft may transfer Customer Data within a geo (e.g., within Europe) for data redundancy or other purposes. For example, Azure replicates Blob and Table data between two regions within the same geo for enhanced data durability in case of a major data center disaster.

Microsoft will not transfer Customer Data outside the geo(s) customer specifies (for example, from Europe to U.S. or from U.S. to Asia) except where necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements; or where customer configures the account to enable such transfer of Customer Data, including through the use of:

Features that do not enable geo selection such as Content Delivery Network (CDN) that provides a global caching service;

Web and Worker Roles, which backup software deployment packages to the United States regardless of deployment geo;

Preview, beta, or other pre-release features that may store or transfer Customer Data to the United States regardless of deployment geo;

Azure Active Directory (except for Access Control), which may store Active Directory Data globally except for the United States (where Active Directory Data remains in the United States) and Europe (where Active Directory Data is in Europe and the United States);

Azure Multi-Factor Authentication, which stores authentication data in the United States;

Azure RemoteApp, which may store end user names and device IP addresses globally, depending on where the end user accesses the service.

Microsoft does not control or limit the geos from which customers or their end users may access Customer Data.

See the E.U. Data Protection Directive section below for information on the regulatory framework under which Microsoft transfers data.

E.U. Data Protection Directive

The E.U. Data Protection Directive (95/46/EC) contains strict requirements for the handling of personal data in the European Union. Under European law, our customer is the data controller of its Customer Data and Microsoft is the data processor. To allow for the flow of information required by international business (including cross border transfer of personal data), Microsoft adhere to the U.S.-EU Safe Harbor Framework developed by the Department of Commerce in coordination with the

European Commission. The Safe Harbor certification allows for the legal transfer of E.U. personal data outside the E.U. to Microsoft for processing.

Microsoft also offers customers E.U. Standard Contractual Clauses that provide additional contractual guarantees around transfers of personal data for in-scope services. Microsoft's implementation of the E.U. model clauses has been validated by European Union data protection authorities as being in line with the rigorous privacy standards that regulate international data transfers by companies operating in its member states. Microsoft is the first company to receive joint approval from the E.U.'s Article 29 Working Party for its strong contractual commitments to comply with E.U. privacy laws no matter where data is located.

It is important to note that Microsoft will transfer E.U. Customer Data outside the E.U. only under very limited circumstances. See the Location of Data section for details.

Customer Data and Other Data Types

Customer Data is all the data, including all text, sound, software or image files that you provide, or are provided on your behalf, to us through your use of the Services. For example, Customer Data includes data that you upload for storage or processing in the Services and applications that you or your end users upload for hosting in the Services. It does not include configuration or technical settings and information.

Administrator Data is the information about administrators (including account contact and subscription administrators) provided during sign-up, purchase, or administration of the Services, such as name, address, phone number, and e-mail address.

Metadata includes configuration and technical settings and information. For example, it includes the disk configuration settings for an Azure Virtual Machine or database design for an Azure SQL Database.

Access Control Data is used to manage access to other types of data or functions within Azure. It includes passwords, security certificates, and other authentication-related data.