EXHIBIT "D"

SECURITY AND DATA PROTECTION

We offer an online cloud (Azure) based platform, developed in .NET technology which is fully managed by a third party (ITERA). Our provider complies with national, international and industry standards relating to security.

We know that due to its complexity, data hosting can be a major concern for many organizations. Therefore, we designed this solution with the aim to assure a dynamic, secure, and efficient distribution of data.

Azzule's solution is based in:

- Web applications and tools that allow users to submit data in defined data forms.
- Web applications and tools that allow users to distribute information according to permission levels.
- Processes that collect, consolidate, and transform information, so we can assure the accuracy of data.

Related information regarding the security models that currently apply to Azure:

- **Management Port and Secure Communication (NGS):**
  You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains *security rules* that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

- **Encryption at rest with platform-managed key (SSE+PMK)**
  Most Azure managed disks are encrypted with Azure Storage encryption, which uses server-side encryption (SSE) to protect your data and to help you meet your organizational security and compliance commitments. Azure Storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud. Disks with encryption at host enabled, however, are not encrypted through Azure Storage. For disks with encryption at host enabled, the server hosting your VM provides the encryption for your data, and that encrypted data flows into Azure Storage.

  Data in Azure managed disks is encrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant.

- **Secure transfer is an option that forces the storage account to accept requests only from secure connections (HTTPS).**
  Using HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as brokers, eavesdropping, and session hijacking.

- **To protect machines from threats and vulnerabilities, a compatible endpoint protection solution is installed**
  Microsoft Defender for Cloud provides health assessments of supported versions of Endpoint protection solutions.

- **Azure Defender for servers**
  Microsoft Defender for servers is one of the enhanced security features of Microsoft Defender for Cloud. Use it to add threat detection and advanced defenses to your Windows and Linux machines whether they're running in Azure, on-premises, or in a multi-cloud environment.

- **Azure Defender for App Services**
  Azure App Service is a fully managed platform for building and hosting your web apps and APIs. Since the platform is fully managed, you don't have to worry about the infrastructure. It provides management, monitoring, and operational insights to meet enterprise-grade performance, security, and compliance requirements.

  Microsoft Defender for App Service uses the scale of the cloud to identify attacks targeting applications running over App Service. Attackers probe web applications to find and exploit weaknesses. Before being routed to specific environments, requests to applications running in Azure go through several gateways, where they're inspected and logged. This data is then used to identify exploits and attackers, and to learn new patterns that will be used later.

- **Azure Defender for SQL Servers**
  Azure Defender for SQL is a unified package for advanced SQL security capabilities. Azure Defender is available for Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics. It includes functionality for surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database. It provides a single go-to location for enabling and managing these capabilities.

- **Azure Defender for Storage**
  Microsoft Defender for Storage is an Azure-native layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit your storage accounts. It utilizes the advanced capabilities of security AI and Microsoft Threat Intelligence to provide contextual security alerts and recommendations.

Security alerts are triggered when anomalous activities occur. These alerts appear in Microsoft Defender for Cloud, and are also sent via email to subscription administrators, with details of suspicious activity and recommendations for how to investigate and remediate threats.

- **Azure Security Center**
  Assess the security state of all cloud resources—including servers, storage, SQL, networks, applications, and workloads—that are running in Azure, on premises, and in other clouds. Visualize security state and improve security posture by using secure score recommendations. View compliance against a wide variety of regulatory or company security requirements by centrally managing security policies. Perform ongoing assessments and get rich, actionable insights and reports to simplify compliance.
  The secure score is shown in the Azure portal pages as a percentage value, but the underlying values are also clearly presented.

  To increase security, review Defender for Cloud's recommendations page for the outstanding actions necessary to raise score. Each recommendation includes instructions to help remediate the specific issue. Recommendations are grouped into security controls. Each control is a logical group of related security recommendations, and reflects vulnerable attack surfaces. Score only improves when you remediate all of the recommendations for a single resource within a control. To see how well organization is securing each individual attack surface, review the scores for each security control.

- **Azure installations, on-premises, and physical security**
  Azure is composed of a globally distributed datacenter infrastructure, supporting thousands of online services and spanning more than 100 highly secure facilities worldwide.

  The infrastructure is designed to bring applications closer to users around the world, preserving data residency, and offering comprehensive compliance and resiliency options for customers. Azure has 58 regions worldwide, and is available in 140 countries/regions.

  A region is a set of datacenters that is interconnected via a massive and resilient network. The network includes content distribution, load balancing, redundancy, and data-link layer encryption by default for all Azure traffic within a region or travelling between regions. With more global regions than any other cloud provider, Azure gives you the flexibility to deploy applications where you need them.

  Azzule's data servers have been specifically configured with "Always-On High Availability" by ITERA's specialists.

- **Hosting Location.** Azzule's servers and data are hosted in Azure region EU2 (East US 2)

- **Network Architecture**
  The Azure network architecture provides connectivity from the Internet to the Azure datacenters. Any workload deployed (IaaS, PaaS, and SaaS) on Azure is leveraging the Azure datacenter network.

  The network architecture of an Azure datacenter consists of the following components: Edge network, Wide area network, Regional gateways network and Datacenter network.

  The above network components are designed to provide maximum availability to support always-on, always-available cloud business. The redundancy is designed and built into the network from the physical aspect all the way up to control protocol.

- **Azure Customer Data Protection**
  Access to customer data by Microsoft operations and support personnel is denied by default. When access to data related to a support case is granted, it is only granted using a just-in-time (JIT) model using policies that are audited and vetted against our compliance and privacy policies. The access-control requirements are established by the following Azure Security Policy:

  - No access to customer data, by default.
  - No user or administrator accounts on customer virtual machines (VMs).
  - Grant the least privilege that's required to complete task; audit and log access requests.

  Azure support personnel are assigned unique corporate Active Directory accounts by Microsoft. Azure relies on Microsoft corporate Active Directory, managed by Microsoft Information Technology (MSIT), to control access to key information systems. Multi-factor authentication is required, and access is granted only from secure consoles.

  All access attempts are monitored and can be displayed via a basic set of reports.

<u>Other information security practices implemented by Azzule Systems:</u>

- **Cloudflare Protection**
  Cloudflare is a global network designed to make everything you connect to the Internet secure, private, fast, and reliable.

  Cloudflare's 100 Tbps network blocks an average of 70 billion threats per day, including some of the largest DDoS attacks ever recorded. Each and every login, request, and response that goes through our network strengthens the machine learning that we apply to detect and block threats at the edge, before they ever reach our organization.

- **Pentesting practices**
  A pentesting is a set of simulated attacks directed at a computer system with a single purpose: to detect possible weaknesses or vulnerabilities so that they are corrected and cannot be exploited. These audits begin with the collection, in open access sources, of information about the company, employees, users, systems and equipment. It continues with an analysis of vulnerabilities that will be exploited, even with social engineering techniques, attacking systems until they achieve their objectives. Finally, a report is made that indicates whether the attacks would be successful, and if so, why and what information or access they would obtain, that is, attacks are simulated as they would be carried out by a cybercriminal who wanted to take control of the system or with the information contained therein. In this way, it can be determined:

  - whether the computer system is vulnerable or not,
  - assess whether your defenses are sufficient and effective, and
  - assess the impact of security flaws that are detected.

- **Code scanning (Sonar)**
  Source code analysis tools, also known as Static Application Security Testing (SAST) Tools, can help analyze source code or compiled versions of code to help find security flaws.

  SAST tools can be added into your IDE. Such tools can help you detect issues during software development. SAST tool feedback can save time and effort, especially when compared to finding vulnerabilities later in the development cycle.

  SonarQube is a Code Quality Assurance tool that collects and analyzes source code, and provides reports for the code quality of your project. It combines static and dynamic analysis tools and enables quality to be measured continually over time.

- **Multifactor Authentication (MAF)**
  Multifactor authentication (MFA) is a security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction. Multifactor authentication combines two or more independent credentials: what the user *knows*, such as a password; what the user *has*, such as a security token; and what the user *is*, by using biometric verification methods.

  The goal of MFA is to create a layered defense that makes it more difficult for an unauthorized person to access a target, such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one or more barriers to breach before successfully breaking into the target.

- **Information security staff trainings**
  Information technology security awareness training educates employees about common scams, like email attachments containing malware, and phishing emails that request personal information. With this kind of security literacy, our employees will be less likely to fall into data breach traps.

- **Database encryption**
  Database encryption can generally be defined as a process that uses an algorithm to transform data stored in a database into "cipher text" that is incomprehensible without first being decrypted. It can therefore be said that the purpose of database encryption is to protect the data stored in a database from being accessed by individuals with potentially "malicious" intentions. The act of encrypting a database also reduces the incentive for individuals to hack the aforementioned database as "meaningless" encrypted data is of little to no use for hackers.

- **DAST Tools**
  Dynamic application security testing (DAST) is one of the many technology groupings of security testing solutions. DAST is a form of black-box security testing, meaning it simulates realistic threats and attacks. This differs from other forms of testing such as static application security testing (SAST), a white-box testing methodology used to examine the source code of an application.

  DAST includes a number of testing components that operate while an application is running.

- **Software Composition Analysis Tools**
  Modern software is assembled using third-party and open source components, glued together in complex and unique ways, and integrated with original code to provide the desired functionality. Third-party (including commercially licensed, proprietary, and “source available” software) along with open source components provide the necessary building blocks that allow organizations to deliver value, improve quality, reduce risk and time-to-market. The benefits of open source are many. However, by using open source components, organizations ultimately take responsibility for code they did not write. Strategic alliances between organizations and open source projects can lead to healthy open source usage and overall risk reduction.

  Component Analysis is the process of identifying potential areas of risk from the use of third-party and open-source software and hardware components. Any component that has the potential to adversely impact cyber supply-chain risk is a candidate for Component Analysis.

- **AI tools and third party legal frameworks**
  Any AI tool to be used is and will be subject to third party tools assessments and tests, as described in some other bullets in this same document. In addition to this measure, any third party services, AI-oriented or not, are and will also be subject to legal framework measures, such as Non-Disclosure Agreements, and other Privacy and Confidentiality agreements, as also Information Security assessments and reviews.

EXHIBIT "D"

SECURITY AND DATA PROTECTION

- **Managed firewalls**
  Managed firewalls protect our services from malicious traffic before it ever touches the servers. Hackers, script-kiddies, and other unscrupulous characters have forced all of us to vigilantly protect our networks.
    - Key features:
        - Source/Destination-based IP/port filtering
        - Port Scan protection
        - ICMP/UDP/SYN flood protection
        - IP address spoofing
        - Malformed packet protection

- **SSL Certificate**
  SSL Certificate confirms for your site visitors that you are an actual business and that it is safe for them to share personal data with your site. Sitting on a secure server, it encrypts data like credit card numbers and other personal information preventing criminals from obtaining it for malicious reasons. It also confirms the identity of the website and the validity of the business, by providing information about the certificate holder, the domain that the certificate is issued to, the Certificate Authority who issued the certificate and the root country it was issued in.
    - Key features:
        - Safely encrypt sensitive or transactional information
        - Prove the authenticity and security of your site

- **Azzule's Disaster Recovery Plan (additional from MS Azure's) and Business Continuity**
  Azzule counts with additional DRP plans in case of MS Azure's total disruption and/or failure, helping ensure business and operations continuity.

  Having cloud infrastructure, Azzule's operation is able to continue from different enabled locations in the US, Mexico and Chile, besides, alternate protocols to enable operations from any other location with internet conection.