[SAMPLE] JURISTECH SOFTWARE AND SYSTEM DESCRIPTION

DOCUMENT CONTROL PAGE

Document ID	SCG/JURSD/121/1.0
Security Classification	Confidential
Date Issued	30-Jul-2025
Version	1.0
Project Name	NA
Author	AJ KHAN

VERSION HISTORY / CHANGE HISTORY

Version	Date Issued	Issued to	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

REVIEWERS

Version	Review Date	Reviewed By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

APPROVERS

Version	Date Approved	Approved By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

DISTRIBUTION LIST

Date	Name / Distribution List	Comments
30-Jul-2025	Customer_DL_ABC	Published to Customer ABC

DOCUMENT CONTROL PAGE

RELATED DOCUMENTS

DOC_ID	DOC Version#	DOC Link	Comments
SCG/BASEINS/005/1.0			Base Template Instructions
SCG/PXF/008/1.0			Policy Exception Form
SCG/S2RAS/113/1.0			SOC2 Asset Scope
SCG/RMF/015/1.0			Risk Management Policy

CONFIDENTIALITY STATEMENT

This document is the exclusive property of [SecureCyberGates]. This document contains proprietary and confidential information. Duplication, Redistribution, or use, in whole or in part, in any form, requires consent of [SecureCyberGates].

[SecureCyberGates] may share this document with auditors under non-disclosure agreements [NDA] to demonstrate Security Audit requirement compliance.

Contents

[Note : This is just sample System description and DOES NOT represent JurisTech Original Systems.]

1) Overview of Operations

At JurisTech, we are more than just a software company; we are a driving force behind the digital transformation of the financial world. As a global leader in enterprise-class lending and recovery solutions, we empower banks, financial institutions, telecommunications, and automotive companies worldwide to thrive in a rapidly evolving landscape.

Our journey began during the turbulence of the 1997 Asian financial crisis, a period that shaped our commitment to innovation and resilience. Since then, we have grown into a pioneer, delivering cutting-edge software solutions that harness the power of artificial intelligence (AI), conversational chatbots, digital onboarding, and more. From loan origination and credit scoring to debt collection and litigation, we partner with banks and financial institutions to redefine the future of finance. Our solutions do not just adapt to change; they drive it. By enabling digital transformation, we ensure our clients provide an unparalleled customer experience while achieving their business goals with confidence.

[Content Copied from publically available resource https://juristech.net/juristech/about-us/]

1.1) Description of Services Provided

Buiseness

Our business goals focus on being globally as well as locally. At JurisTech, we offer our in-house specialists to align with our client's goal; either in understanding the Malaysian Shariah's law, or complex compliance process of international regulation. At the very heart of JurisTech, we believe in identifying the root cause of a business issue in order to come up with a befitting solution. With a multinational workforce, we are sensitive to the diverse customer's journey and aim to bring our best game in software implementation in the Fintech industry.

Product Design and Development: Our R&D and product teams put innovation at the heart of our solutions, ensuring every product conforms to the market standards.

Project Delivery Capability: We offer extensive support for pre, during, and post-project implementation to ensure the client's goals are met and fulfilled.

International Delivery Capabilities: Our sustainable and agile business operations, processes, and decision-making has been strategically optimised to cater to the international market with different time zones.

Financial Industry Knowledge and Expertise/ Tech Leader: Headed by See Wai Hun, JurisTech's visionary CEO (also named as EY Woman Entrepreneur Of The Year 2019 in

Malaysia), our team of financial and tech experts diligently fulfil client's requirements to not only transform your existing system but also revolutionise your digital processes.

Governance & Compliance: One of the advantages of working with us is our in-house specialists' expertise on Islamic banking and Shariah compliance regulations, on top of being sensitive to local regulations where the project is implemented or based at.

Quality Assurance Service/Quality Management: Quality control and management during a system implementation are critical aspects in ensuring every project is executed successfully. We ensure every implementation is managed thoroughly for the highest quality assurance and deliverables.

[Copied from publically available resource https://juristech.net/juristech/our-capabilities/]

Technical

JurisTech prides itself on its technical innovation across all our solutions over the years. JurisTech's solutions are designed and developed using the Juris Solutions Interaction Platform (JSIP) which is built on-top of the Juris Application Server (JAS). JAS consists of an integrated framework of highly scalable components which is used to build enterprise-strength solutions.

JurisTech's technical capabilities have many times proven to set highly competitive standards to all our clients to create seamless and secure service streams across their customer channels. With our technology, we aim to deliver the best-in-class solutions to serve our clients operational excellence.

Low Code Technology Our solutions are supported by powerful front-end frameworks that do not require advanced coding capabilities.

Powerful Workflow Engine Our solutions are backed with a robust infrastructure, Juris Workflow Engine, engineered with the flexibility to manage and design different workflows that accommodate different target markets (banks/non-banks).

Multi-channel Integration and API-powered Our solutions enable straight-through processing capabilities and are inclusive of the entire digital ecosystem in the market.

Multi-tenancy Control Our solutions come with multiple tenancy controls on all major tables such as user access matrixes, user management, user workflows and applications with the ability to segregate each tenancy with its own setups and data in a single instance.

Application Security Juris SecureGuard Security Framework was built to uphold security measures and encrypt customer sensitive information against threats such as Input Filtering of XSS, SQL Injection attacks, DDoS attacks, Cross-site scripting across all our

solutions. Juris SecureGuard also conforms with all regulatory requirements in every region.

Disaster Recovery Our solutions run on systematic protocols to overturn several different adversities such as network outages, transaction rollbacks, and out of memory errors.

[Copied from publically available resource https://juristech.net/juristech/our-capabilities/]

Delivery and Support

We appreciate the complexity of every project implementation and always strive to deliver our best in supporting our clients' transformation. We understand behind every successful project execution; it is crucial to ensure sufficient post-project support for a smooth transition.

Help Desk Our cooperative help desk personnel are always ready to walk you through any pertaining issues at any stage of the project lifecycle, making sure your support needs are met and fulfilled.

Advocates for Client Experience and Success (ACES) Back up by an extensive team of technical personnel with diverse knowledge of the industry from our HQ assisted by our off-site team in Uganda, we offer end-to-end post-implementation guidelines to help you navigate through your newly enhanced system based on project requirements, organisational needs, etc.

Training & Resources Training and resources are adequately given and delivered throughout the project implementation and post-execution to support your transition into the newly implemented system.

Service Level Agreement Client satisfaction is always at the top of our priorities; we fulfil our obligations and deliver on our promises 100%. We strive to achieve mutual understanding in terms of performance standards to establish a positive experience for all involved parties.

[Copied from publically available resource https://juristech.net/juristech/our-capabilities/]

2) List of Products

[Copied from publically available resource https://juristech.net/juristech/solutions/]

Digital Onboarding

Product Name	Description
Juris Access	Juris Access is a digital customer onboarding platform, that enables

	financial institutions or companies to create an engaging end-to-end onboarding journey. Built to accelerate your customers' financial-related applications, Juris Access digitally onboards them by facilitating customer acquisition, application, eligibility pre-screening, and evaluation for financial and credit products. https://juristech.net/juristech/juris-access/
Juris DecisionCraft	Juris DecisionCraft is an auto-decisioning engine that orchestrates and synergises different data and analytics from different systems or sources to produce the best decision possible. https://juristech.net/juristech/juris-decisioncraft/
Juris V-Box	Juris V-Box is an instant, secure document request and collaboration platform, that enables financial institutions or agents/partners to request, collect, track and secure customers' documents. https://juristech.net/juristech/juris-v-box/
Juris Anny	Juris Anny is an intelligent chatbot with natural language processing (NLP) specifically engineered to cater to financial service-related questions and transactional requests. https://juristech.net/juristech/juris-anny/
Financial Services Marketing	Specialised marketing solutions for financial services providers https://juristech.net/juristech/financial-services-marketing/

[Copied from publically available resource https://juristech.net/juristech/solutions/]

Digital Lending

Product Name	Description
Juris Origination	Juris Origination is a loan origination system that automates the entire loan application and approval process. The system drastically simplifies the process from application, scoring, evaluation, underwriting, approval, acceptance, documentation, up to disbursement. https://juristech.net/juristech/juris-origination/
Juris Credit	Juris Credit is a credit administration platform that unifies and manages the entire credit process workflow of valuers, solicitors and financial institutions in a single platform. https://juristech.net/juristech/juris-credit/
Juris Analyst	Juris Analyst is a financial evaluation system for businesses that simulates, evaluates, and forecasts your clients' financial health and their repayment ability. It provides data feed to scoring and risk rating systems and intelligently analyses company financial positions over a desired period, including the past, present and future. https://juristech.net/juristech/juris-analyst/
Juris OneCore	Juris OneCore is an end-to-end loan management solution that is built

	with small and medium-size lenders in mind, empowering these businesses to effectively manage loan or financing products offerings. It is built to encompass the full lifecycle of loan management, including application creation, reconciliations, loan rescheduling, loan settlements and write-offs. https://juristech.net/juristech/juris-onecore/
Juris Leads	Juris Leads is a lead management system that captures, tracks, and nurtures prospects and existing customers, to be converted into new business opportunities. It captures leads from multiple channels and sources, automatically distributes to the right relationship manager and create a centralised platform to manage prospects and customers' conversion journey. https://juristech.net/juristech/juris-leads/

[Copied from publically available resource https://juristech.net/juristech/solutions/]

Collection and Recovery

Product Name	Description
Juris Collect	Juris Collect is an end-to-end enterprise debt collection system that handles early delinquent accounts to late-stage accounts, whilst intelligently employing personalised collection strategies for different customer profiles. https://juristech.net/juristech/juris-collect/
Juris Legal	Juris Legal is a legal workflow management platform for late-stage recovery, connecting financial institutions and law firms. It helps financial institutions to streamline and optimise the standard civil suit and foreclosure litigation processes by automating case distribution, billing and approval processes, and most importantly, providing a platform for law firms to collaborate real-time on litigation matters. https://juristech.net/juristech/juris-legal/
Juris Predator	Juris Predator is an all-in-one computer-telephony integration (CTI) software equipped with powerful diallers, inbound call routing and comprehensive information tracking. It is able to turn your computer into a telephone call management system centralising control over all call-related tasks with powerful and intelligent outbound dialling modes options – preview, progressive and predictive dialling. https://juristech.net/juristech/juris-predator/
Nexcoll	The one-stop software solution for debt collection agencies — with web-based access that lets you login from anywhere, anytime! https://nexcoll.my/nexcoll/
Collectxpress	Cloud-based collection software that manages and keeps track of all your invoices without ever missing a customer's payment. https://collectxpress.net/

[Copied from publically available resource https://juristech.net/juristech/solutions/]

Artificial Intelligence

Product Name	Description
Juris AICraft	Juris AICraft is an Agentic AI platform that integrates diverse AI capabilities to deliver tailored solutions for your evolving business needs. Each AI technology operates as independent modules, collaborating like specialised agents to solve complex business challenges. https://juristech.net/juristech/juris-aicraft/
Juris MindCraft	Juris Mindcraft is an automated Machine Learning (autoML) and artificial intelligence (AI) platform that uses advanced machine learning (ML) techniques to build powerful AI models. An effortless AI that enables enterprises especially banks and financial institutions to make intelligent business decisions and gain insights to solve real-world problems. https://juristech.net/juristech/juris-mindcraft/
Juris Spectrum	Juris Spectrum is an end-to-end digital banking platform, offering a unique, holistic digital banking experience for customers and businesses. Powered by connectivity and agility, Juris Spectrum is composed of a robust digital core and state-of-the-art customer engagement, lending, deposits, and collection capabilities. https://juristech.net/juristech/juris-spectrum/

[Copied from publically available resource https://juristech.net/juristech/solutions/]

3) Principal Service Commitments and System Requirements

JurisTech designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that JurisTech makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that JurisTech has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- The fundamental design of JurisTech's software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
- JurisTech implements various procedures and processes to control access to the production environment and the supporting infrastructure.
- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.
- Internal and External Regular vulnerability scans over the system and network, and penetration tests over the production environment; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between JurisTech and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans and,
- Operational procedures supporting the achievement of availability commitments to user entities.

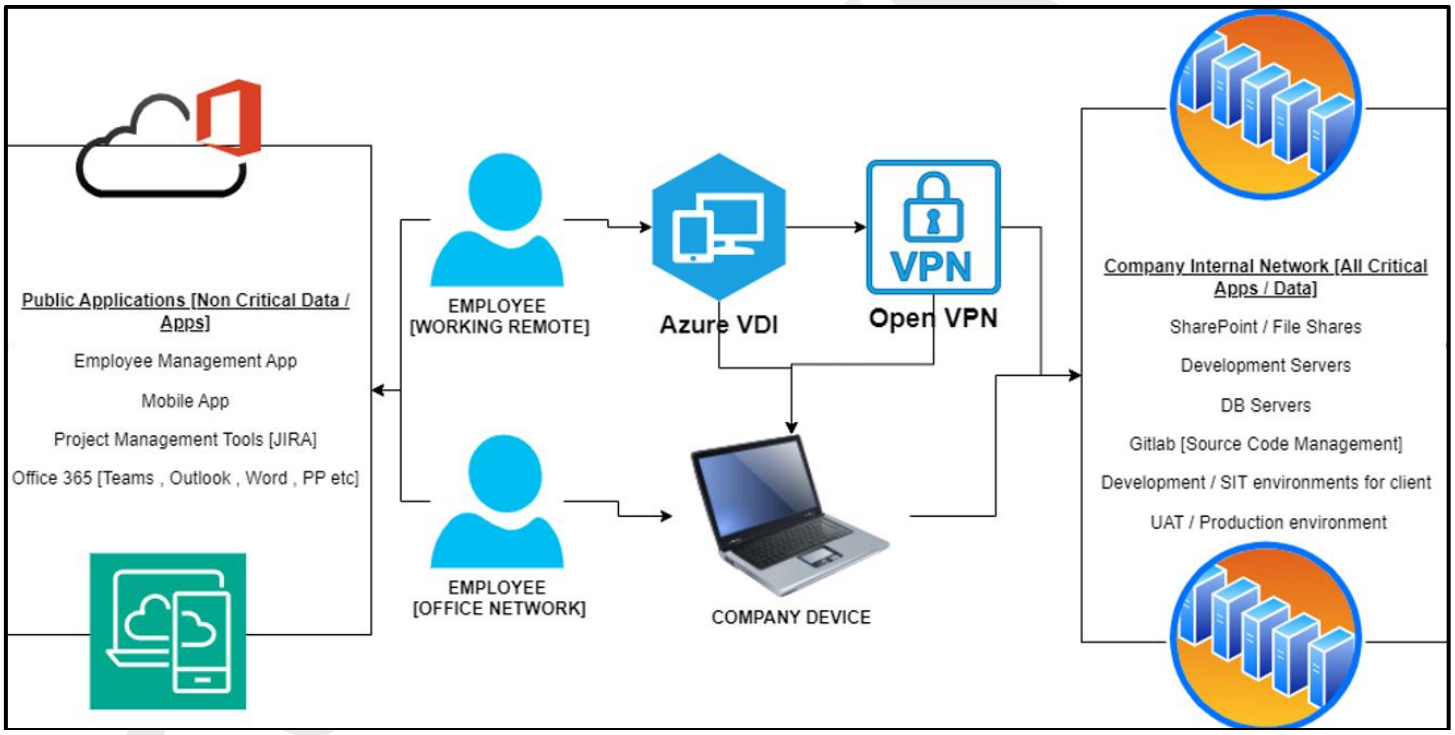
Such requirements are communicated in JurisTech 's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

4) Components of the System used to provide services

The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below:

- **Infrastructure**
- **Software**
- **People**
- **Data**
- **Policies and Procedures**

4.1) Infrastructure



NOTE: This diagram is just a sample one and does NOT represent JurisTech

Company Data is hosted on Premise [e.g. Development Servers, Internal applications like Employee management [Employee Attendance, Their Details, Leaves etc.]

Some Company Data is hosted on Cloud e.g. Company uses JIRA Cloud , Some data on Azure Cloud, Some on AWS cloud , Company uses Office 365 products for daily Communication]

Customer Data is managed by Customers. e.g. JurisTech develop Loan management Software and deliver the product to Customer [Now all Production Data is responsibility of Customer] . Some of these cients have asked JursTech to handle their own Customer data for this JurisTech uses Azure , AWS , Google and Oracle Cloud

4.2) Software

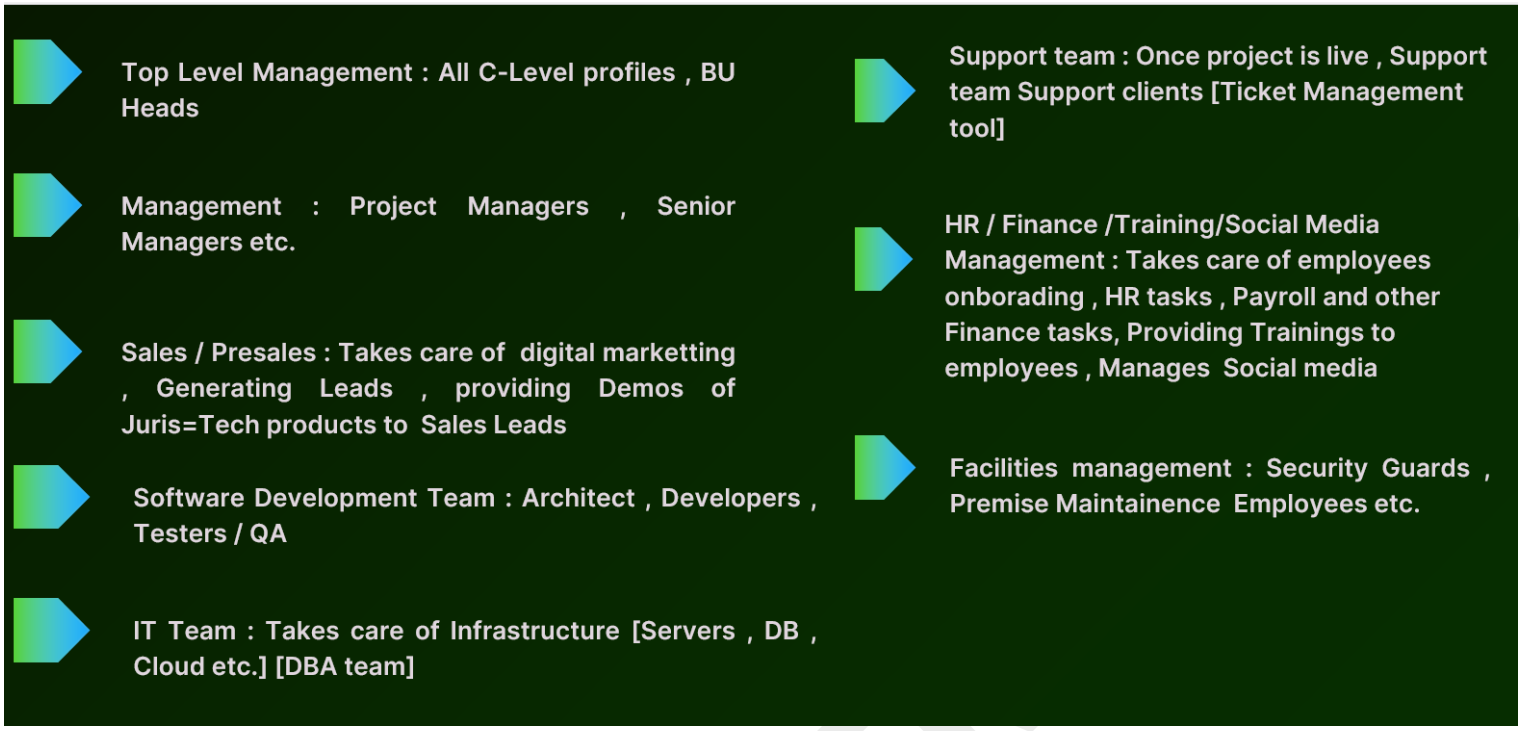
Kindly refer List of products at https://juristech.net/juristech/solutions/

Technical Security Controls

TOOLS AND TECHNOLOGIES	
Office Communication	Office 365 Suite [Teams]
VPN	Open VPN
Employee Management [Employee Attendance Records , Leave System , Employee details]	In House Web and Mobile Applications
Support Tool / Ticketing Tool	Internal Help Desk Website [Accessible over Internet for all Clients]
DevOps Tools	GitHub Enterprise [On Premise Version / Self Managed] , Visual Studio Code , Docker , Microsoft Data Protection Manager backups
AntiVirus	McAfee Total Protection | Antivirus software
Cloud / On prem	Development Server VMs on premise [Inside Company Office Building , Server Machines with Microsoft Server OS and Hyper-V] , UAT / Production Servers for Some client managed on Oracle / Azure [Azure VDI for Remote Employees]
Project Management	JIRA

Tool used	Description
Microsoft Threat Modeling Tool	Threat modelling at design Phase.
GitHub CodeQL	GitHub SAST (Static Application Security Testing)
Sonatype Nexus IQ	Open-source vulnerabilities
BurpSuite	DAST tool
OWASP ZAP	DAST tool
Azure Sentinel	SIEM and SOAR tool
Azure /AWS/ Oracle WAF	Web application Firewall
Cisco Secure Firewall 4200 Series	Physical firewall for Office-premise network
OWASP TOP 10	Approach for Security Testing

4.3) People



4.4) Data

Data, as defined by JurisTech, constitutes the following:

- Company Data [All Data related to Company Phone number, email Ids etc.]
- Customer Data [Any data specific to customer, customer details, Projects etc.]
- Application Data [Source code, Project Documents, Reports etc.]
- Environment details [Development, SIT/UAT, Production environment details etc.]
- System files
- Audit and Error logs

Any Confidential Data / Reports delivered externally are only sent using a secure method—encrypted email, secure FTP, or secure websites to customer users.

All data that is managed, processed and stored as a part of the JurisTech software application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value and criticality to achieving the objectives of the organization.

All customer data is categorized as confidential. Further, all customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples

Customer Confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	• Customer system and operating data • Customer PII • Anything subject to a confidentiality agreement with a customer
Company Confidential	Information that originated or is owned internally, or was entrusted to JurisTech by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general public.	• JurisTech's PII • Unpublished financial information • Documents and processes explicitly marked as confidential • Unpublished goals, forecasts, and initiatives marked as confidential • Pricing/marketing and other undisclosed strategies
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	• Press releases • Public website

Customer data is retained per agreements with customers and disposed of upon request by customers. A confirmation is sent back to the customer to notify them that the disposal is complete

4.5) Policies and Procedures

Formal policies and procedures have been established to support the JurisTech software application. These policies cover:

- ✓ Code of Business Conduct
- ✓ Change Management
- ✓ Data Retention
- ✓ Data Backup
- ✓ Information security
- ✓ Vendor management
- ✓ Physical security
- ✓ Risk management
- ✓ Password
- ✓ Media disposal

- ✓ Incident management
- ✓ Endpoint security
- ✓ Encryption
- ✓ Disaster recovery
- ✓ Data classification
- ✓ Confidentiality
- ✓ Business continuity
- ✓ Access control
- ✓ Acceptable usage
- ✓ Vulnerability management
- ✓ Human Resource Management

All policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

JurisTech also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the JurisTech software application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

5) Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part JurisTech 's description of the system. This section provides information about the five interrelated components of internal control at JurisTech, including:

- ✓ Control environment
- ✓ Risk assessment
- ✓ Control activities
- ✓ Information and communication
- ✓ Monitoring controls

5.1) Control environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of JurisTech's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of JurisTech's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

JurisTech and its management team has established the following controls to incorporate ethical values throughout the organization:

- ✓ A formally documented "Code of business conduct" communicates the organization's values and behavioral standards to staff members
- ✓ Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- ✓ All new employees go through background checks as a part of the hiring process.

Commitment to Competence

JurisTech's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.

- ✓ Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- ✓ Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- ✓ Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

Senior Management Oversight

JurisTech's control awareness is significantly influenced by its senior management. Attributes that define "tone at the top" include senior management's experience of its

members, their involvement and scrutiny of operational activities, and their interaction with independent assessments of the company's operations and information security posture.

Management Philosophy and Operating Style

JurisTech's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to monitoring business risks, and management's attitudes toward personnel and the processing of information. JurisTech's control environment reflects the philosophy of management. JurisTech 's information security function, composed of senior management and the Information Security Officer, meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

Specific control activities JurisTech has implemented in this area are described below:

- ✓ Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- ✓ Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment, and high severity security incidents annually.
- ✓ Senior management meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap.

Organizational Structure and Assignment of Authority and Responsibility

JurisTech's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

The management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and updated as required.

Human Resources

JurisTech's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the management's ability to hire and retain top quality personnel who ensure the service organization operates at maximum efficiency.

Specific control activities that the service organization has implemented in this area are described below:

- ✓ Background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- ✓ Job positions are supported by job descriptions.
- ✓ New employees are required to acknowledge company policy and confidentiality related agreements upon hire and annually thereafter.
- ✓ Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- ✓ Performance evaluations for each employee are performed on an annual basis.
- ✓ If an employee violates the Code of Conduct in the employee handbook or the company's
- ✓ Policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.

5.2) Risk assessment

JurisTech regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to the applicable trust services criteria set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

JurisTech's risk assessment process identifies significant risks inherent in products and services as they oversee their areas of responsibility. JurisTech identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks. This process identifies risks to the services provided by the JurisTech Software application, Data, Infrastructure and management has implemented various measures designed to manage these risks

JurisTech believes that effective risk management is based on the following principles:

- ✓ Senior management's commitment to the security of JurisTech assets [Software, Data, Infra, Documents etc.]
- ✓ The involvement, cooperation, and insight of all JurisTech staff.
- ✓ Initiating risk assessments with discovery and identification of risks.
- ✓ Thorough analysis of identified risks.
- ✓ Commitment to the strategy and treatment of identified risks.

- ✓ Communicating all identified risks to the senior management.
- ✓ Encouraging all JurisTech staff to report risks and threat vectors.

Scope

The risk assessment and management program applies to all systems and data that are a part of the JurisTech assets [Software, Data, Infra, Documents etc.]. The JurisTech risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of JurisTech's Information Security Officer and the department or individuals responsible for the area being assessed. All JurisTech staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment

JurisTech uses a number of vendors to meet its business objectives. JurisTech understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

JurisTech employs several activities to effectively manage their vendors. Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, JurisTech assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support JurisTech's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, JurisTech management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix**,** which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment

As part of the design and operation of the system, JurisTech identifies the specific risks that service commitments may not be met, and designs controls necessary to address those risks. JurisTech's management performs an annual Risk Assessment Exercise to identify

and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity and mitigating action.

5.3) Control activities

JurisTech's control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Logical Access Control

The JurisTech software application uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

JurisTech has identified certain systems that are critical to meet its service commitments. All access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems are revoked within three business days.

Administrator access to the production console is restricted to authorized system and security administrators. Powerful service/system accounts and keys are either restricted from direct user authentication or authorized to unique users through a password vault or equivalent security solution. Production infrastructure root level account usage is logged with alerting configured.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assesses the appropriateness of the access and permission levels and make modifications based on the principle of least-privilege, whenever necessary.
Staff members must use complex passwords, wherever possible, for all of their accounts that have access to JurisTech customer data. Staff are encouraged to use passwords which have at least 12 characters, randomly generated, alphanumeric and special-character based. Password configuration settings are documented and systematically enforced based on the password complexity requirements configured on each critical system. Access to cloud services or remote access systems requires multi-factor authentication (MFA). Additionally, company owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

Physical Access and Environmental Controls

JurisTech has a well-rounded physicals security in place to protect the site, the equipment and underlying software from any physical damage such as vandalism, theft and other accidents. The business suite that houses our office as well as our own premises has 24-hour CCTV surveillance and controlled access. Only authorized personnel can enter the office premises, and this is validated via a bio-metric access system. All individual laptops and workstations are password protected and the responsibility of JurisTech employees. The servers and other systems maintained by JurisTech are in a secure environment and not all employees are provided access. Only authorized and relevant users with need-to-have access are allowed. Smoke detectors and relevant fire suppression systems are in place and periodically tested and go through maintenance cycles. Overall, physical security measures are taken care of by both the building management and JurisTech.

Incident Management

JurisTech has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact JurisTech via support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools [Juris Gold] consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- ✓ **Low severity incidents** are those that do not require immediate remediation. These typically include a partial service of JurisTech being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.
- ✓ **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium severity incidents usually cover the large majority of incidents found.
- ✓ **High severity incidents** are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, malicious access of business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed and immediate remediation steps should begin.
- ✓ **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

Network Operations Monitoring

Web applications are protected by deploying network firewalls and security groups that inspect traffic flowing to the web application for common attacks. The network is segmented based on the label or classification level of the information stored on the servers. Incidents and alerts from the security utilities are reviewed by FIS and Security team. Security events requiring further investigation are tracked using internal ticketing systems and monitored until resolved.

JurisTech only uses network ports, protocols, and services listening on a system with validated business need to run on each system. Default-deny rules drop traffic except those services and ports that are explicitly allowed.

Cryptography

User requests to JurisTech's systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority. Remote system administration access to JurisTech web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using strong algorithms like Advanced Encryption Standard (AES) 256 bit.

Change Management

A documented Change Management Policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the JurisTech are reviewed, deployed, and managed. The policy covers all changes made to the JurisTech software application, regardless of their size, scope, or potential impact.

The Change Management Policy is designed to mitigate the risks of:

- ✓ Corrupted or destroyed information
- ✓ Degraded or disrupted software application performance
- ✓ Productivity loss
- ✓ Introduction of software bugs, configuration errors, vulnerabilities, etc.

The ability to implement changes into the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities. ServiceNow software are used for change request management. Customer content and personal information are not used in non-production environments.

Software Security Assurance

Secure coding practices are established based on the programming language and development environment used. In-house developed software includes explicit error checking and documented inputs, including for size, data type, and acceptable ranges or

formats. Security analysis is performed to verify secure coding practices are followed during change control. Vulnerabilities identified, if any, are tracked to resolution.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

Vulnerability Management

Vulnerability scanning tools are used to scan systems on the application, network to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities.

Endpoint Management

Endpoint management solutions are in place that include policy enforcement on company issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include encryption on devices for data at rest.

To help prevent malware, the following are implemented within the organization:

- ✓ Anti-malware software [McaFee] to continuously monitor and defend each of the organization's workstations and servers.

Availability

JurisTech has a documented business continuity plan (BCP) and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). Frequent Backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

5.4) Information and Communication

JurisTech maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, JurisTech also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff via the company intranet.

Information about the system and services are maintained and made available to users on the company website.

5.5) Monitoring controls

JurisTech's management monitors controls to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored.

This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Disclosure of Incidents

There were no system incidents as of **JANUARY 01 2025 to JUNE 15th 2025**, requiring disclosure that either:

Were the result of controls failing; or,

Resulted in a significant impairment to the achievement of system requirements or service commitments to customers.

Complementary User Entity Controls

JurisTech's controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for JurisTech customers.

For customers to rely on the information processed through the JurisTech's software application, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- ✓ User entity is responsible for managing their organization's JurisTech's Products account as well as establishing any customized security solutions or automated processes through the use of setup features
- ✓ User entity is responsible for protecting established user IDs and passwords within their organizations.
- ✓ User entity is responsible for reviewing customer access to the JurisTech's Products application periodically to validate appropriateness of access levels.
- ✓ User entity is responsible for approving and creating new user access to the JurisTech's Products Software application.
- ✓ User entity is responsible for removing terminated employee access to the JurisTech's Products software application.
- ✓ User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the JurisTech's Products software application.
- ✓ User entity is responsible for sending data to JurisTech's software application via a secure connection and/or the data should be encrypted.

- ✓ User entity is responsible for notifying JurisTech's Products software application if they detect or suspect a security incident related to the JurisTech
- ✓ User entity is responsible for reviewing email and other forms of communications from JurisTech related to changes that may affect JurisTech customers and users, and their security or availability obligations.
- ✓ User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the system.
- ✓ User entity is responsible for endpoint protection of workstations used to access the system.
- ✓ User entity is responsible for developing their own business continuity and disaster recovery plan.

[Note : This is just sample System description and DOES NOT represent JurisTech Original Systems.]

SECURE CYBER GATES

THANKYOU!
FOR CYBER-SECURITY RELATED UPDATES, KINDLY FOLLOW BELOW PAGES...

https://www.linkedin.com/in/aj57/
https://www.linkedin.com/company/securecybergates
https://securecybergates.com/services
https://www.youtube.com/@SecureCyberGates
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com

SECURE CYBER GATES