LEGALEASE SOLUTIONS

Data Security Architecture Outline

LEGALEASE SOLUTIONS

User Authentication

- All users authenticate through a VPN with an HTTPS access line using 256-bit encryption
- All users have 2-factor authentication which enables access to all our work environments
- VPN is connected using a firewall featuring an Intrusion Prevention System (IPS) and Intrusion Detection System (IDS)
- The firewall logs all activity from connected devices for monitoring and analysis purposes
- Mobile users have Mobile Device Management (MDM) installed on their devices

Communication Channel: Office 365

- Office 365 provides secure communication and collaboration tools
- Office 365 Security Features:
    - Utilizes Azure Active Directory (AD) for user authentication and access control
    - Enables encryption for data in transit using Transport Layer Security (TLS)

Data Security Best Practices

- End-to-end encryption for transmitted and stored data
- Regular audit and monitoring of security logs
- Security awareness training for employees to prevent social engineering attacks
- Regular vulnerability assessments and patch management to address security vulnerabilities
- Incident response plan in place to effectively respond to security incidents

Data Access Methods

Sharing Data

- Users share data using Transport Layer Security (TLS), or SCP over HTTPS
- Users have separate logins with strong passwords and Multi-Factor Authentication (MFA) for enhanced security

Uploading Documents via NDA Portal (AWS)

The NDA Portal is hosted on Amazon Web Services (AWS) with integrated security features

AWS Security Measures:

- Utilizes AWS Identity and Access Management (IAM) to manage user access and permissions
- Implements AWS Key Management Service (KMS) for encryption key management
- Integrates with Azure 0Auth for trusted users' access and user control
- Stores data in Amazon S3 buckets with server-side encryption (SSE) enabled
- Utilizes AWS Shield for DDoS protection and AWS WAF for web application firewall
- The NDA Portal integrates with Azure Active Directory (Azure AD) for user authentication via 0Auth

Classification of Data

Strictly Confidential

This includes the most sensitive information that requires the highest level of protection.
Access is strictly limited to authorized personnel on a need-to-know basis.

- Employee Personally Identifiable Information (PII) such as social security numbers, passport numbers, or biometric data
- Financial records including payroll information, bank account details, or credit card numbers
- Intellectual property (IP) such as trade secrets, product designs, or proprietary algorithms
- Legal documents containing sensitive information related to litigation, contracts, or IP rights

Confidential

This category includes critical information that requires protection from unauthorized access or disclosure.
It is vital for the organization's operation and security.

- Customer databases that include personal information like names, addresses, and phone numbers
- Business plans and strategies for future initiatives or expansion
- Research and development documents outlining new product ideas or technological innovations
- Internal memos discussing organizational changes or sensitive operational procedures

Classification of Data

Internal

The public category of data includes information that can be accessed by the public. While not as sensitive as confidential data, it still requires controlled access.

- Employee directories and organizational charts
- Meeting agendas and minutes for internal team meetings
- Training materials and resources for employee development programs
- Internal policies and procedures manuals for employee reference

Public

The public category of data includes information that can be accessed by the public. It does not contain sensitive or proprietary information.

- Marketing materials such as brochures, advertisements, or press releases
- Publicly available reports or publications
- General website content including company news, events, or product information
- Social media posts or updates intended for public consumption

Strictly Confidential

Owner

Authorized Personnel

Confidential

Owner

Authorized Personnel

Reviewer/Authorized vendors

Internal

Owner

Internal Team Members

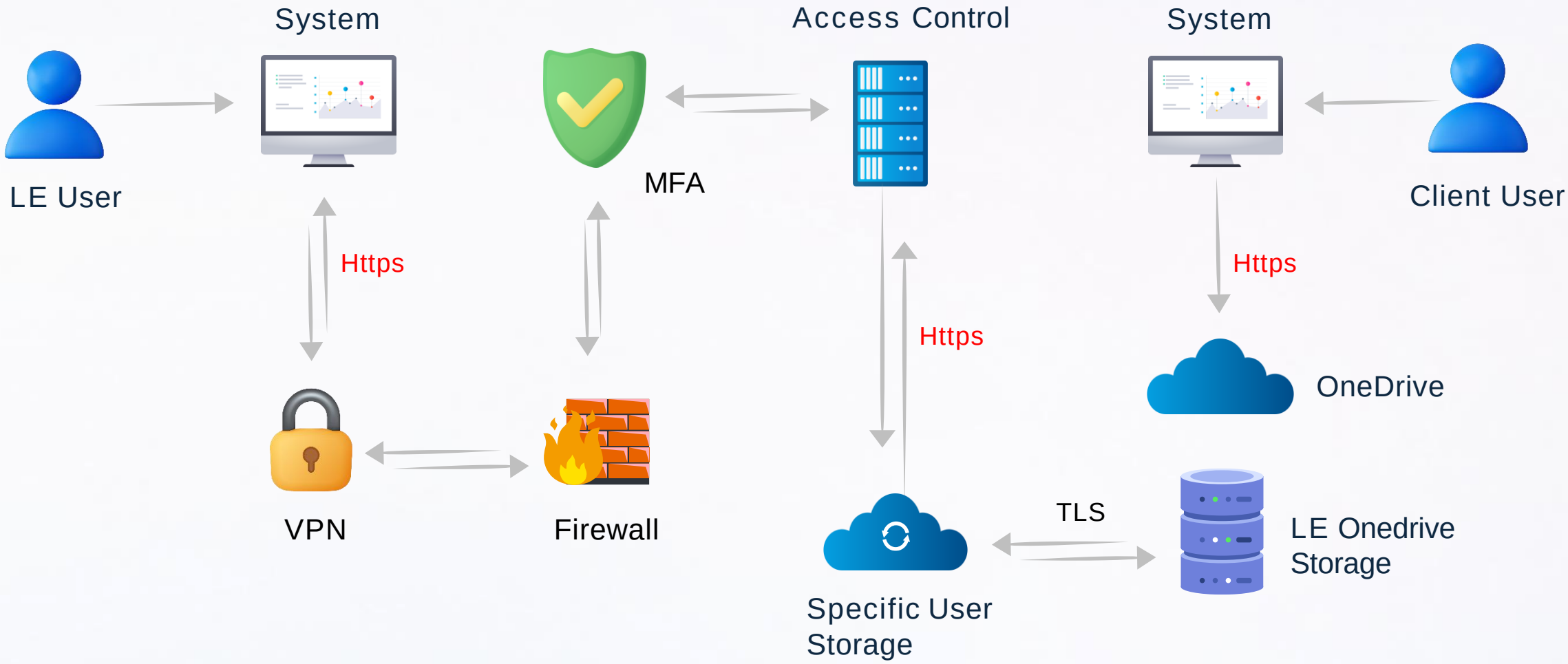
Public

Owner

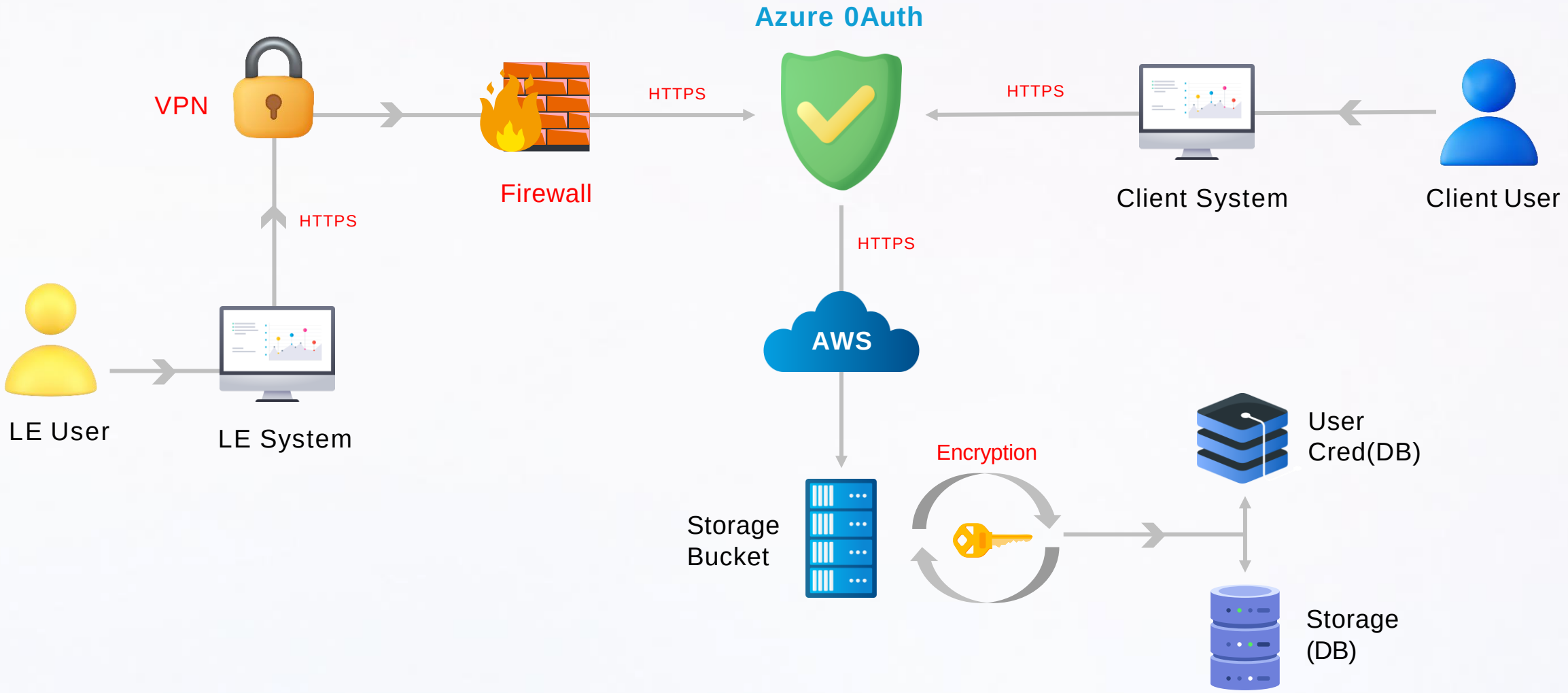
Public Users

LEGALEASE SOLUTIONS

LegalEase Office 365 Environment



LegalEase NDA Portal



How Data is Received (Data Reception)

When data is received, it is automatically owned by the PE (Project Engineering) team.

Storage and Access Management

- All client data is uploaded to dedicated storage spaces on OneDrive
- The PE (Project Engineering) team owns data and manages access for the Delivery team members according to project-based roles
- The Operations team owns all the client-side contracts and manages access for the Client Success and Executive teams

Encryption and Backup

- Data is stored using standard Microsoft encryption protection
- Integrated with Office 365 backup solution to ensure daily backup of all data

Data Retention

All data has a standard retention period of at least 365 days. Retention periods may vary based on the nature and importance of the data.

Data Destruction Process

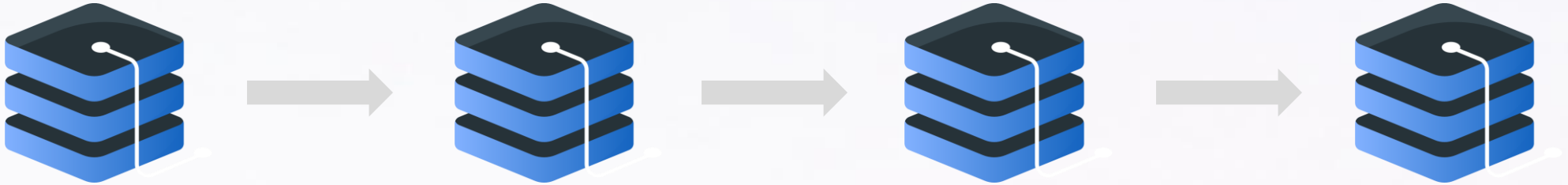
After the data retention period, all client data is securely removed from the portal.

Data Reception

Storage and Access Management

Encryption and Backup

Data Retention



Data Reception

(Owned by PE team)

Access based on roles/services

Standard retention period of at least 365 days

Data Destruction Process

Secure removal after the retention period expires

LEGALEASE SOLUTIONS