Luware
Nimbus

Data Security and Privacy White Paper

Document-ID	LUNIM-INFOSEC
Version	2.1
Status	Approved
Issue Date	01.08.2024
Valid from	15.09.2024
Valid to	Sabrina Deakin, COO

Luware AG
Pfingstweidstrasse 102
CH-8005 Zürich

solutions@luware.com
+41 58 404 28 00

Luware

Contents

Document-ID	LUNIM-INFOSEC
Version	2.1
Status	Approved
Issue Date	01.08.2024
Valid from	15.09.2024
Valid to	Until new version is published
Approvals	Sabrina Deakin, COO

Luware AG
Pfingstweidstrasse 102
CH-8005 Zürich

solutions@luware.com
+41 58 404 28 00

Luware

1 Introduction

Luware Nimbus is a cloud-based Software-as-a-Service (SaaS) product that enables the delivery of seamless and reliable customer service. To ensure optimal performance, security, and compliance, Luware implements a comprehensive cloud security strategy.

This document outlines the implementation of this strategy and forms an integral part of the Luware Cloud Services Terms of Use including the Luware Data Processing Agreement, as updated occasionally, or customers' individual agreement with Luware, as applicable.

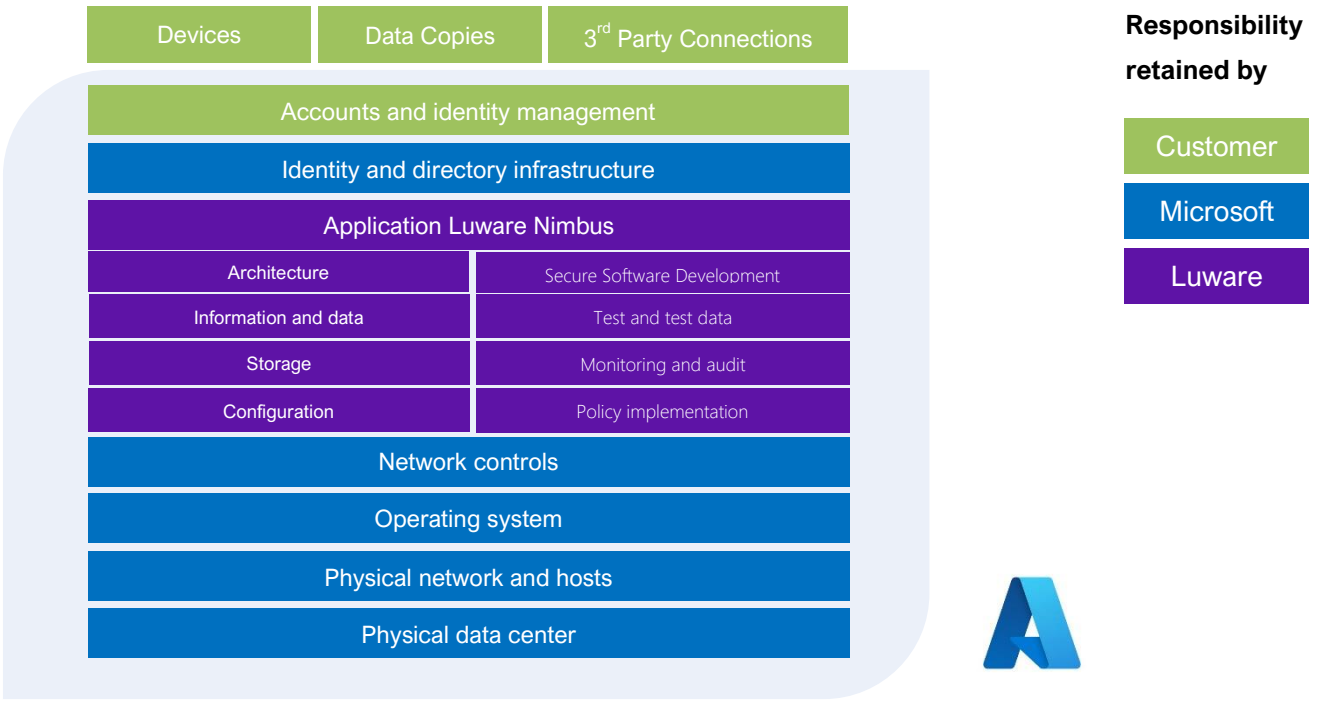
This document is aimed at our current and prospective Luware Nimbus customers as well as authorized technology partner.

2 Security Scope and Responsibilities

Luware Nimbus is a Microsoft Teams application developed on the Extend Model and hosted in the Microsoft Azure cloud. Multiple layers of system security are covered by Microsoft and Azure Security Services. This cloud security concept is called the *Shared Responsibility Model.*

Whilst Luware manages security controls for the whole application layer, including the development tools and storage options on the Azure platform, customers have a significant role to play in ensuring security and data protection. Customers are required to manage their accounts and identities, devices, data backups and third-party connections such as custom integrations. These are the areas where customers have sole control and responsibility over their data and security.

In addition, customers are responsible for ensuring that data provided from external third-party systems to Luware Nimbus, such as custom parameters for displaying customer information, can compliantly be used and stored in the Luware Nimbus Conversation Context) for the duration of the retention period.



3 Authentication and Access

In accordance with SOC 2 Type II security requirements, the Luware Nimbus platform is protected against unauthorized access and data breach. Some of these requirements, such as multifactor authentication, are a fundamental building block of the Luware Nimbus security architecture, along with tight integration with the Microsoft's authentication platform.

Luware Nimbus is a licensed-user platform, where only specific, named individuals or members of a licensed team are given access to consume the service.

3.1 Authentication

User access is authenticated with tight integration to Microsoft's global identity management platform (Microsoft Entra ID) and industry standard authentication. Luware recommends using the OAUTH 2.0 authentication with Microsoft Entra ID.

3.1.1 Multi-Factor Authentication

Multifactor authentication (MFA) is recommended and can be enabled by the customer. This is achieved by leveraging Microsoft Entra ID multifactor authentication (MFA). Currently, Luware Nimbus does not support any other MFA providers.

3.1.2 Anonymous Access

Anonymous access is not supported.

3.1.3 Generic User Accounts

Generic service and administration user accounts are not permitted. End-customer users are only granted application-specific account roles / permissions, tied to their named Microsoft Entra account. This ensures that customers maintain complete control over their user account security in line with their organizational requirements.

3.1.4 Application Service Accounts

All internal application service accounts are provisioned on a per-application basis, with enforcement of minimal permissions. Service Account details are protected, conforming to industry security standards. Examples for such Service Accounts:

- Power Automate User
- PowerBI User

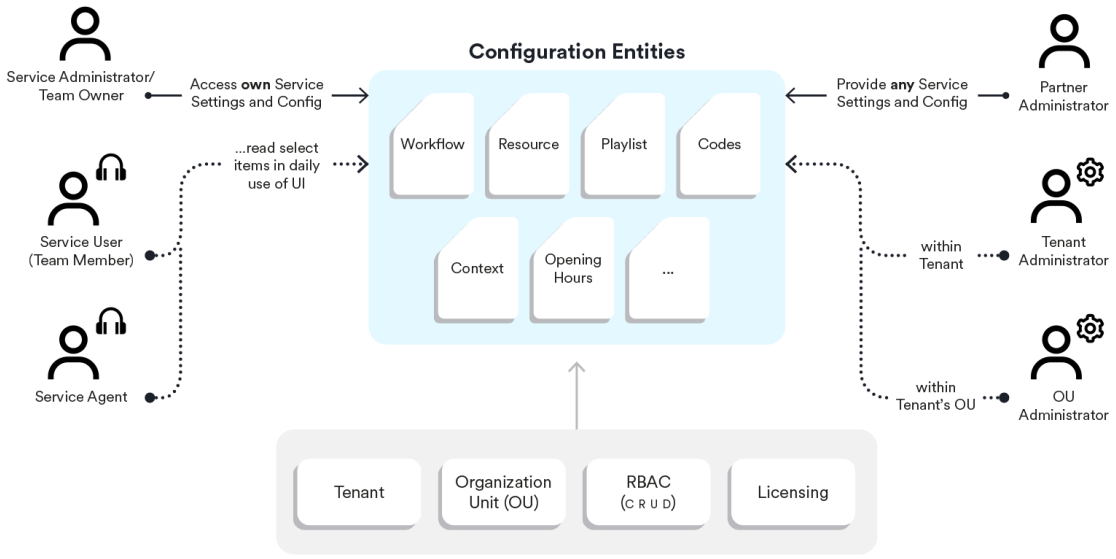
3.1.5 Extended Presence Accounts

Luware Nimbus uses various criteria, including the user's presence states, to route tasks. To access basic user states, Luware Nimbus uses a setting called "External Access". This enables Luware Nimbus to see the users' simple presence states (Available, Busy, Away, Do Not Disturb, Offline), without having to access more detailed statuses like "Busy → In a Call" or "Busy → In a Conference".

Customers can opt to use guest user presence accounts. These accounts, though optional, allow Luware Nimbus to access extended user presence status. These presence accounts should not use MFA for protection. Instead, Luware recommends the use of conditional access to secure these accounts.

3.2 Role-Based Access

Administrative users that require access to operate the platform (both from a customer and Luware system administration perspective) must have their administrative permissions explicitly granted and are only given the minimal level of access enforced via Role-based Access Control (RBAC). The customer, or its technology partner, perform self-administration for access to data by leveraging predefined RBAC policies provided for by Luware Nimbus.



Access and Permission concept

3.3 Administrative Access

Luware uses the following domain concept to manage the system.

- **System Access.**
  This highest access level of a deployment is controlled by a Microsoft Entra group. Only Luware employees can be assigned ***System Administrator*** roles using dedicated Admin accounts. With these Admin accounts they can manage all tenant settings within the specified Luware Nimbus cluster they are granted access to.

  On this level, Luware leverages the following technical security rules:
  - **Principle of Least Privilege:** Luware follows the principle of least privilege and 'need to know'. Luware personnel are only allowed to access data that is necessary for them to fulfil their current roles and responsibilities.
  - **Regular Data Access Review:** There is a regular review process in place to assess and correct any unnecessary access privileges. This ensures that access is kept in line with role requirements.
  - **Formal Access Request Process:** If someone needs additional access beyond their current permissions, a formal access request process is followed.
  - **Access is technically restricted** to compliant and managed devices owned by Luware. Accounts are technically restricted from logging in from countries outside the EEA and countries with a valid adequacy decision of the EU Commission.

- **Tenant Access.** A tenant is a dedicated instance of Luware Nimbus, connected to the Office 365 tenant of a single customer (identified by its O365 tenant ID). All users, settings, and services of a Luware Nimbus instance (for a single customer) are stored and managed in that tenant. At tenant level, the customer can add an administrative Microsoft Entra group whose members are granted permission to manage the tenant as ***Tenant Administrators***. They manage data access via Luware Nimbus roles, monitor tasks and configure tenant wide settings.

  It is the customer's sole responsibility to maintain and control access within their organization and Luware Nimbus tenant(s).

- **Partner Access.** If a customer uses a partner to manage their Luware Nimbus tenant, the partner and its employees who require access, must be registered within the tenant configuration. To achieve this, the partner creates an administrative group in their Microsoft Entra ID and adds the users requiring access to this group in the customer tenant. The customer's ***Tenant Administrator*** adds the GUID of this group as a ***Partner Administration Security Group*** in the settings of the tenant.

  If a Tenant Administrator requires support, a ticket can be issued with Luware Support. If requested and instructed by the customer via Luware's ticketing portal, a ***System Administrator*** can add the GUID of the Partner Administrative Security Group to the tenant configuration. This will grant members of the Partner Administration Security Group the ability to manage the

assigned tenant and its configuration. The members of this group will have access to manage the customers' Luware Nimbus environment and are responsible for controlling data access, administrative roles, and privileges within their organization and for the customer's tenant.

The granting of access to a partner is the customer's sole consideration and remains the customer's sole responsibility throughout the deployment.

The customer's Tenant Administrator can restrict the partner access to the following data groups:

- Allow Partner to see User Identifiers
- Allow Partner to see Customer Identifiers

- **Team Access.** For Luware Nimbus Advanced or Enterprise Routing services, users are part of a Microsoft Teams team. ***Team Owners*** can manage the team and the configuration of the Luware Nimbus service line.

3.4 User Access

Users are added to the tenant by the ***Tenant Administrator*** using the Microsoft Entra ID. ***Tenant Administrators*** can assign more granular Luware Nimbus RBAC roles to Nimbus users and grant them more privileges within the Luware Nimbus system, such as the role of service supervisor, which can configure a Luware Nimbus service line. Luware's Role Access Concept (luware.com) describes the RBAC matrix in Luware Nimbus.
Agents are employees that serve a Luware Nimbus service line. Agents must be Microsoft Teams users with a valid telephony license. The assignment of to a service line depends on the service type.

- For Luware Nimbus Advanced or Enterprise Routing services, agents are assigned to a Luware Nimbus service line through their team membership in Microsoft Teams by the ***Team Owner***.
- For Luware Nimbus Contact Center services, agents are assigned to a service line based on their skill configuration and the applicable distribution policy.

3.5 Access Monitoring and Change History

Detailed access logging on the customer level is leveraging Entra ID sign-in logs within the customer tenant. Microsoft Azure Sentinel is used as a centralised logging solution for all user access activities. Event logs are retained for 12 months and will not be made available to customers.

System Administrators, Partner Administrators and Tenant Administrators have read access to the Change History starting in 2024. In the Change History customers find a list of relevant changes made to the configuration within a certain tenant. The log data is retained for a period of at least 6 months and a maximum of 24 months.

4 Operational Security

4.1 Security Baseline

Luware's security baseline applies guidance from the Microsoft cloud security benchmark version 1. The Microsoft cloud security benchmark provides recommendations on how to secure a cloud platform. Based on this, Luware has established a security baseline completing regular internal security reviews. It defines the minimum standard as well as guidelines on implementation and maintenance. It includes a set of documentation outlining reference architecture, system hardening procedures, implementation guides, and security principles that must be adhered to when implementing, upgrading, migrating, or decommissioning a system within the Luware Nimbus infrastructure.

Luware's security baseline is frequently reviewed and updated to adjust to changing business needs, evolving technology, emerging market requirements and threat landscapes.

4.2 Threat Prevention

Luware implements policies, tools, and technology to protect the Luware Nimbus environment from both external and internal threats. Luware Nimbus utilizes Microsoft's security stack, mainly its Azure Well-Architected Framework security pillar. Using this Azure framework, Luware implements the state-of-art security delivered in Azure data centers globally relying on the technology that is built with customized hardware, integrated security controls into the hardware and firmware components, and added protections against threats such as DDoS. As part of this approach Luware makes use of additional Azure services such as Defender for containers, Log Analytics Workspaces and Azure Sentinel.

Furthermore, Luware leverages Microsoft WAF, the cloud-native service that protects Luware Nimbus against common web exploits using OWASP core rule sets. It provides complete visibility into the environment and blocks malicious attacks.

4.3 Secure Software Development

Luware has implemented Secure Software Development practices including, obligatory security awareness trainings for software developers, secure design principles, defined coding practices and automatic security auditing for every new software build. Within the development pipeline, Luware covers a large array of automated tests prior to production deployment. These tests include RBAC role access verification.
The Secure Software Development process is reviewed on an annual basis and updated as needed.

4.4 Patching and Roadmap

Luware maintains a regular patch cycle to keep the Luware Nimbus platform up to date and protected against vulnerabilities. These patch cycles are generally executed within maintenance windows which are communicated to the customer in advance.

The roadmap is divided into blocks (e.g. bi-annually or quarterly). These blocks consist of several sprints. The roadmap planning and order of implementation follows a defined feature management procedure to keep a refined view on expected development effort, feature prioritization and impediments towards the release plan.

Major release is the default form of release. It consists of prioritized roadmap items in a completed state. Minor releases usually follow a major release. They contain hotfixes, bugfixes and smaller enhancements.

4.5 Incident Response

Luware has implemented processes to respond to and manage incidents as they occur. System monitoring and alerting tools are in place to proactively detect incidents in the Luware Nimbus infrastructure. The Service Desk is equipped to respond to incidents reported directly by customers.

Critical incident review is part of Luware's security operations policy. Incident causes and outcomes are reviewed quarterly by the Security Operations team to identify process gaps, training needs, or required documentation updates or improvements. Corrective actions are implemented as necessary.

4.6 Change Control

To minimize operational risks resulting in data exposure, service degradation or unavailability, Luware maintains a change management process that controls all non-standard changes made to a production system. All changes that impact a production system are documented, tested, and approved by a Change Approval Board prior to deployment.

Change management tools are used to reflect this process and record the multiple stages of changes including creation, design, documentation, approval, and outcome. All system employees are required to submit a change request on a change management tool, detailing any changes to in-scope platforms and systems. All changes are raised before implementation. For emergencies, service-affecting situations, an emergency change must be retrospectively raised and approved.

The change management process is reviewed annually and updated if changes are required.

4.7 Physical Security

Luware Nimbus is hosted in Microsoft Azure public cloud infrastructure Microsoft takes a layered approach to physical security.

Access to the physical data center facilities is tightly controlled by outer and inner perimeters, with increasing security at each level. Security measures include perimeter fencing, security guards, locked server racks, integrated alarm systems, 24-hour video surveillance in the operations center, and multi-factor access control. Only authorized personnel are granted access to Microsoft's data centers. Logical access to Microsoft 365 infrastructure, including customer data, is prohibited from within Microsoft data centers.

Microsoft's Security Operations Centers use video surveillance along with integrated electronic access control systems to monitor data center sites and facilities. Cameras are positioned to effectively cover the facility perimeter, entrances, shipping bays, server cages, interior aisles, and other sensitive security points. As part of their layered security posture, any unauthorized entry attempts detected by the integrated security systems generate alerts to security personnel for immediate response and remediation.

These layers include:

- **Access request and approval:** access must be requested prior to arriving at the datacentre. A valid business justification for the visit must be presented.
- **Visitor access:** all visitors that have approved access to the data center are accompanied by a member of staff.
- **Facility's perimeter:** before entering the data center, visitors must go through a well-defined access point.
- **Building entrance:** the data center entrance is staffed with security officers who have undergone training and background checks. These security officers routinely patrol the data center and monitor the videos of cameras inside the data center.
- **Inside the building:** 2FA is required to move throughout the data center. Once identity is validated, access to an area to which access has been pre-approved is granted.
- **Data center floor:** visitors are only allowed onto the floor that they've been approved to enter. A full body metal detection screening is mandatory. Additionally, video cameras monitor the front and back of every server rack.

Luware's Legal and Compliance team regularly reviews Microsoft Azure's SOC2 Type II audit reports including any bridge letters. This ensures adequate measures can be taken should a control activity fall short of the expected quality standards and may materially impact Luware's security operations.

4.8 Logical Security

Access to systems and data within Luware Nimbus is restricted based on a stringent and hardened role-based access control system enforced over multiple system layers from the virtualization layer through

to the operating system layer and into the end user application. Where in Luware's control, the logical access and security controls are controlled in a pre-defined security framework with regular reviews and a Joiner/Mover/Leaver process. Our Joiner/Mover/Leaver and User review processes are closely aligned with our SOC2 control processes.

5 Data Privacy & Processing

By using Luware Nimbus, customers consent to the processing according to the Luware Cloud Services Terms of Use and Luware Data Processing Agreement, or the individual agreement entered into between the customer and Luware, as applicable. This framework includes provisions for lawful and fair processing of personal data, purpose limitation, data minimization, accuracy, storage limitation, and accountability. It also includes provisions on data subjects' rights as well as data breach notification and handling requirements. It provides customers with adequate, legally binding provisions on data privacy and security in accordance with applicable law.

Sections set out below are to be understood in the context of this contractual framework set out above and serve as an overview for customers to understand the technicalities of personal data handling.

5.1 Data Locations

Luware Nimbus is hosted on Microsoft Azure. The hosting instances are located in Switzerland, the UK and Germany, as chosen by the customer. Microsoft Azure was chosen due to the service's outstanding security, resiliency, and connectivity practices.

5.1.1 Switzerland

There are two Luware Nimbus instances in Switzerland (CH01 and CH02) hosted in the Microsoft Azure Data Center located in Switzerland, with the primary data center being Microsoft Azure Switzerland North (Zurich) and the secondary data center (DR, backup location) being Microsoft Azure Switzerland West (Geneva).

5.1.2 Germany

There are two Luware Nimbus instances in Germany (DE01 and DE02) hosted in the Microsoft Azure Data Center Region Germany West, located in Germany, with the primary data center being Microsoft Azure Germany West Central (Frankfurt) and the secondary data center (DR, backup location) being Microsoft Azure Germany North (Berlin).

5.1.3 United Kingdom

The Luware Nimbus instance United Kingdom is hosted in the Microsoft Azure Data Center located in the UK, with the primary data center Microsoft Azure UK South (London) and the secondary data center (DR, backup location) being Microsoft Azure UK West (Cardiff).

5.1.4 EU Cluster

The Luware Nimbus instance Europe is hosted in the Microsoft Azure Data Center Europe West located in the Netherlands (Amsterdam).

5.1.5 Australian Cluster

The Luware Nimbus instance Australia (AU01, AU02) is hosted in the Microsoft Azure Data Center New South Wales.

5.1.6 US Cluster

The Luware Nimbus instance US (US01, US02) is hosted in the Microsoft Azure Data Center East US (Virginia).

5.2 Multihoming

With the multihoming feature, customers have the option to add more tenants to different Luware Nimbus clusters after having been onboarded to a chosen primary cluster. With multihoming, Luware syncs relevant data to a separate Cosmos DB which is spread over all cluster regions available, now or in the future. The data we sync is:

Field	Description
UserID	Distinct GUID of the user within Nimbus
Office365ID	GUID of the user in Office 365 tenant of the customer
TenantID	The GUID of the customer's Office 365 Tenant
LocationID	The string with the full name of the cluster, in which a user is homed

If a user is added to a Microsoft Teams Team within Office 365 which is configured with Advanced Routing or Enterprise Routing in a region where the user is not homed, the user is not assigned and is marked as "unsynchronized" in the local database.
For the duration of the customer environment enabled on multihoming, data stated above will stay in the Cosmos DB. Multihoming can be disabled only if the primary tenant (main cluster) is left in use. Please raise a support ticket (support@luware.com) to disable Multihoming from your tenant.

5.3 Data Subjects

When using Luware Nimbus, Luware processes personal data of customers, their service users as well as their end-users (e.g. caller ID).

5.4 Type of Data Processed

The table Data Types - Processing, Erasure and Retention outlines the types of personal data being processed when using Luware Nimbus.

5.5 Data Subject Rights

Luware adheres to the GDPR principles of the Right to be Informed, the Right of Access, the Right of Erasure, the Right of Restricting Processing, the Right to Object and the Right to withdraw Consent. In some cases, these rights may be limited due to applicable law. Details are set out in our Luware Data Processing Agreement and Luware Privacy Policy.

Should Luware receive a data subject request on behalf of a customer being the data controller, the request is forwarded to the controller. In some instances, customers can change or delete their data themselves, however this is not the case for all requests. Therefore, if instructed by the customer as the data controller, Luware acts upon requests which are to be sent via the support (support@luware.com) channel.

Data Types - Processing, Erasure and Retention outlines each data subject and the corresponding erasure process.

5.6 Data Disposal

Where reasonably possible and legally permitted, Customer Data is removed from Luware's storage infrastructure 30 days after contract termination. Any backups are automatically deleted one day after backup retention expires.

5.7 Data Processing and Retention

Data within the Luware Nimbus application is retained for the purpose of system operation and reporting. Standard retention policies are in place to ensure data isn't kept any longer than necessary to service its purpose.

Customers are solely responsible for the correctness, accuracy and lawfulness of information they put in or store in their Luware Nimbus tenant. This includes making the necessary disclosures and obtaining consent, if required, before providing information. This particularly applies to information that is provided to and processed within a Customer's Luware Nimbus tenant in the scenarios described in Chapter 9.3.

The defined data retention period cannot be customized. Customers wanting to keep the reporting data longer can archive the data into their own infrastructure.

The retention period per data type can be found in Data Types - Processing, Erasure and Retention.

5.8 Third-Party Processors

Microsoft Ireland Operations Limited.
Luware Nimbus is implemented on the Microsoft Azure cloud environment. Microsoft Azure complies with all EU guidelines, in particular the GDPR. This includes the implementation of Standard Contractual Clauses. Microsoft has implemented the Processor-to-Processor clauses (P2P SCCs) included in Module III of the SCCs. By having Microsoft entities sign the P2P SCCs as both data importer and exporter, Microsoft confers a direct benefit on the customer by assuming increased compliance responsibilities for data transfers.

Amongst numerous other certifications and reports, Microsoft is audited against SOC 2 Type II principles and has an ISO 27001 certification.

Luware Affiliates. Services related to Luware Nimbus such as support, maintenance and development are performed from Luware affiliate locations in Switzerland, the UK and the EU. Both Switzerland and the UK hold a valid adequacy decision by the EU Commission.

No other third parties are directly involved in the provision of services to customers.

Internal Business Infrastructure. Please refer to the Luware Privacy Policy for more information.

5.9 Group Data Protection Officer

The Data Protection Officer for all Luware group companies can be contacted via compliance@luware.com. Applicable references must be made according to the Luware Privacy Policy.

5.10 Data Protection

5.10.1 Protection of Data at Rest

All **backend databases** containing sensitive data (configuration data, reporting data, transaction records) are encrypted using transparent database encryption (AES256).

Any customer data stored at rest within the Luware Nimbus environment underlies the following security measures.

- **Physical Access Control**
- **Logical Access control**: only named individuals with the necessary access privileges can access the logical data storage.

Luware uses the Azure provided **Platform Managed Key** to encrypt the data at rest.

5.10.2 Protection of Data in Transit

Any **information** transmitted between Luware Nimbus and the end customer via public networks is encrypted using strong public key encryption.

Any system **API's** are secured with a token-based authentication system. Access to APIs is logically segregated within the system backend based on the same mechanism as the Web Applications.

5.10.3 Data Segregation

To ensure that customer data is handled securely, logical access controls are enabled. All customer configuration and reporting data, including voice messages, are stored and maintained in the shared Luware Nimbus infrastructure which is logically segregated by the individual Luware Nimbus applications to keep the data demarcated, private and secure.

5.10.4 Data Redundancy

Luware uses geographically distributed data centers in Azure to comply with local legislation, minimize network latency, and enable geo-redundant backup and failover. This means that Azure provides geographical redundancy of the data center itself. Each data center has several zones, and depending on the data center, it can have more zones or less.

Direct data disks holding customer data are configured with local redundancy. Locally redundant storage (LRS) replicates customer data three times within a single data center in the selected region. LRS protects data against server rack and drive failures.

6 Business Continuity Management

Businesses of varying sizes, relay on Luware Nimbus to ensure effective communication across their organization. Due to the nature of the offered service, business continuity planning and testing plays a vital part in providing this service to customers.

This chapter provides an overview of Luware's business continuity measures on the Luware Nimbus platform.

6.1 Business Continuity Program

Luware has implemented a Business Continuity Program (BCP) specifically for Luware Nimbus. Via the risk management process, resources that are critical to maintain operation including people, processes, and technology have been identified. As part of this program, plans are created for each critical business function pertaining to the operation and support of the Luware Nimbus platform.

The established BCPs are internal documents and processes that outline the procedures, detailed steps and all necessary information for the continuation and restoration of critical business processes and systems in the event that various resources become unavailable including the loss of premises, infrastructure, human resources, data and equipment. These documents and processes are confidential and can therefore not be shared with external parties for reasons of data security, confidentiality, and protection of intellectual property.

BCPs are reviewed, tested, and approved by the respective teams and coordinated by the respective team-leads in conjunction with Security Operations. All BCP plans are tested at least on an annual basis, but where applicable more often (for example, during system upgrades, patch-cycles or backup/restore exercises). Relevant gaps, learnings and findings are tracked to resolution in Luware's process management system.

6.2 Risk Management

Luware conducts an annual group-wide risk assessment to identify and evaluate key risks to general business operations and services. By assigning subject-matter experts to each risk category, we ensure that evaluations are thorough and transparent enabling Luware's Group Management and the Board of Directors to take informed decisions for the organisation.

We continually monitor emerging risks, changes to existing categorizations and risk ratings and the status of risk mitigation plans. The process is owned and overseen by Legal and Compliance.

6.3 Security Incident Management

Luware follows a defined Incident Management process conforming to SOC2 security standards. The process provides guidelines, assigns roles and responsibilities and information on how to respond to and communicate any security incidents and system failures.

An incident management tool is used to log security incidents. The category and priority of a security incident is determined as part of the incident management process. Security incidents are verified by Security Operations monthly and assigned to the applicable incident owner who evaluates the root cause and assigns remedial actions. Implementation of actions are tracked by Security Operations.

The health status of the system is generally available on the Luware status page (https://status.luware.cloud). The incident team coordinates and analyses the situation and reports frequently on the status. Where customers are affected, they will be informed immediately.

Security Operations reviews the security incident management process annually and if required, makes necessary changes.

6.4 Incident Response

Luware has developed incident response protocols that include triggers and escalation criteria based on the severity of an incident. This consists of processes for activating plans, assembling recovery teams, and making critical decisions to deal with and remediate any incidents.

The Incident Response Team consists of selected Luware employees who act as the Incident Manager for any incidents that occur. All team members can be the first point of contact in the case of an incident, regardless of the platform or product. This process has been designed to acknowledge that the "most ideal" person to act as the Incident Manager at the point of identification may not be available, and time is crucial in our response. Therefore, the first available person in this team accepts the responsibility to act as the Incident Manager until such a time as a more appropriate Incident Response Team Member becomes available and a handover can take place.

Incidents may span over long time periods, and this is likely to include evenings, night times and weekends, therefore having the ability to ensure multiple people are skilled and trained to take over the management of any individual incident allows Luware to ensure that a handover can take place to ensure full focus and attention to the incident.

6.5 Crisis Management

A crisis management plan is in place to govern a global response following an incident impacting Luware. The plan includes the assembly of a core team of leaders and procedures for fast decision-making and timely communications.

6.6 Third-Party Assurance

Luware evaluates the business continuity capabilities of key vendors and third parties through a vendor assessment process overseen by Legal and Compliance. Key vendors such as Microsoft, are assessed quarterly against their performance by the Supplier Relationship Manager. Any actions resulting from such assessments are tracked until resolved.

7 High Availability and Disaster Recovery

7.1 Definition

Luware adopts the following definition of Business Continuity derived from the ISO 22301 standard: “The capability of the business to continue the delivery of products and services at acceptable, predefined levels following a business disruption.”

7.2 Resilient System Architecture

Luware Nimbus is built on a highly scalable microservice architecture which is configured and optimized to be resilient against service outages with features such as automatic healing and seamless state recovery, auto-scale and auto-restart in case of a failure. Due to the distributed nature of a microservice based application, failures of single components only have minor effects on the stability of the general system. Luware Nimbus services run in the primary data centers of the Azure regions outlined in the Data Location chapter. In case of a full data center outage, the services will be restored to the secondary Azure data center within the selected region and service can resume within the Recovery Time Objective (RTO).

7.3 Database Resilience

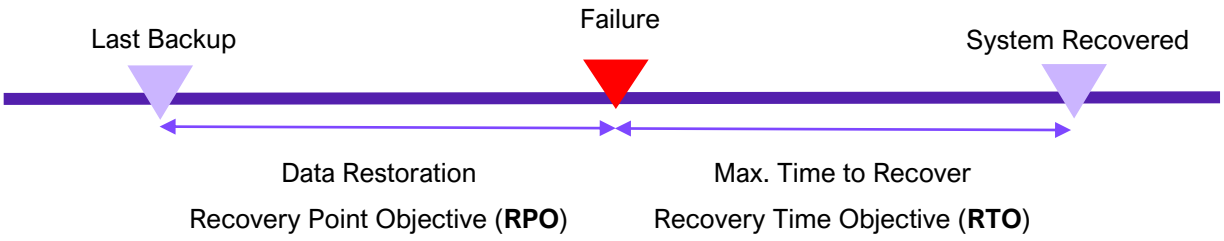
Critical application data is stored in databases that are replicated in near real-time across multiple database instances within the same Azure data center. In case of failure of the primary database or the full data center, the application will be failed over to a database backup in the secondary data center within the region.

7.4 Backup and Restore

Production databases are backed up to the secondary Azure data center within a region to protect the availability of Luware Nimbus in the event of a location-specific catastrophic event. Luware also retains a full backup copy of production data in a remote location significantly distant from the location of the primary operating environment but within the same geographical region/jurisdiction. Full backups are saved to this remote location at least once per day and incremental backups are saved in 60-minutes intervals.

7.4.1 RPO and RTO Backup and Restore Strategy

Due to the resilient design as well as the chosen infrastructure and Backup and Restore strategy, recovery times after the failure of key Luware Nimbus components can be kept to a minimum. The below RPO and RTO are defined for the Luware Nimbus service.



Measure	Description	Data Type	Objective
Recovery Point Objective (RPO)	A measure of tolerance of data loss in terms of time, i.e. the duration of time for which data loss is acceptable.	Data at Rest (configuration and reporting data)	60 minutes based on the last available transactional database backup and subject to Microsoft Azure load management.
Recovery Time Objective (RTO)	A measure of how much time can elapse before full recovery, i.e. the maximum length of time within which a business process must be restored after a disruption.	Any	120 minutes for a system failover to secondary Azure data center and subject to Microsoft Azure load management.

Backups are stored on Azure storage accounts. These storage accounts are configured with local redundant storage (LRS) and an immutable blob policy. LRS replicates the data three times in the local data center. If for example a backup turns out to be defective, this leaves the redundancy of the backup guaranteed.

Access to the storage accounts is monitored and only approved for dedicated employees. Backups therefore have the least access authorization according to the "Least Privilege principle". Backups are stored separately from the actual data and can be archived, for example, through a media break.

Each cluster's backups are **monitored** by Luware's monitoring platform. Any errors are alerted on, and corrective action is taken.

Changes to the recovery process are validated by carrying out the change and restore process. All recovery testing is reviewed by a third party and documented in a comprehensible manner, in particular whether the maximum recovery time is met or not.

8 Further Organizational Measures

8.1 General IT Infrastructure

Critical core IT Infrastructure for the day-to-day operations of Luware including e-mail, telephony, CRM and ERP systems are designed in a resilient fashion with most of those systems being cloud-hosted or pure SaaS solutions. This ensures that in a disaster scenario where business premises or a single data center is lost, Luware is still able to fully operate its business remotely. The necessary security measures are in place to ensure the safety and security when working remotely, including MFA and access to sensitive data via corporate VPN.

8.2 People

Luware operates with a geographically dispersed workforce with locations in Switzerland, United Kingdom and the EU (Germany, Poland and Spain). Luware ensures that system critical roles have substitutes in place with the necessary skills and expertise to take over the day-to-day operations in case of a local emergency. Processes, procedures, and systems of mission critical roles are designed in a way that they can be executed remotely without having physical access to Luware premises.

8.2.1 Background Checks

Luware performs background checks on every System Employee within the company as permitted by local law. The range of background checks performed depends on the role the person holds as well as the level of access they need to perform their daily work. Background checks may include but are not limited to criminal history checks, adverse financials checks, education verification as well as employment history verification.

8.2.2 Security Awareness

All Luware employees undergo regular security awareness training starting with the onboarding process followed up by regular refresher courses and online trainings during the year. Based on the role as well as the level of access an employee needs for their daily work, the level and depth of security awareness training differs. Training topics include secure coding, scam and fraud awareness, general secure working practices, risk awareness, compliance and regulatory adherence training.

8.2.3 Basic principles for Luware User Accounts

Luware has two types of user accounts: the “employee account” and the “privileged account”. For system administrative tasks, users will be provided with a privileged account.

Each user account is personal, non-transferable, and can only be used by the assigned employee. Luware enforces MFA for all types of user accounts.

Passwords must be created according to Luware’s password policy, which includes complexity rules. Passwords for privileged users require a higher level of protection. Therefore, it is prohibited to use pins with those accounts.

Access to Luware IT infrastructure is technically restricted to compliant and managed devices owned by Luware. For applications that manage confidential or secret information, access must be regulated by individual user permissions.

8.3 Audit Reports and Certifications

Luware Nimbus is annually audited by an independent external third party on adherence to **Security Organizational Controls (SOC) 2 Type II** trust service criteria relating to **Security**.

Additionally, **Luware AG** is certified according to **ISO 27001** and **ISO 9001** standards. Any processes related to these standards are rolled out group wide including all affiliate locations. Luware annually conducts an internal as well as an external audit regarding adherence to these standards.

8.3.1 Security Organizational Controls 2 - Type II

A SOC 2 Type 2 report is an internal controls report capturing how a company safeguards customer data and how well those controls are operating. This report is based on the **AICPA's Trust Services Criteria** (TSC) and is currently conducted by PWC. It provides an independent, third-party assessment of the controls that an organization has implemented with regards to the audited TSC. Luware is audited within the scope of the anticipated trust service criteria for **Security**.

Details of the SOC 2 Type II report are strictly confidential and are provided to selected customers upon request and subject to signature of a separate non-disclosure agreement. Luware will provide a letter of confirmation of the report to customers upon request which is to be issued with the responsible sales representative.

8.3.2 ISO 27001

ISO 27001 provides guidelines to manage the confidentiality, integrity, and availability of information assets by assessing and controlling associated risks. It outlines requirements for an information security

management system (ISMS), encompassing policies, procedures, and controls to safeguard data like personal, intellectual, and financial information. It aids in risk identification, data breach prevention, and effective response to security incidents by managing information security risks.

Luware AG's current ISO 27001 certification is provided to customers upon request via the responsible sales representative.

8.3.3 ISO 9001

ISO 9001 is an international standard that sets out the requirements for a quality management system (QMS) within an organization. It provides a framework for organizations to establish, maintain and continually improve data security and privacy practices requiring organizations to identify, assess and manage risks related to information security. This includes implementing appropriate controls to protect against unauthorized access, theft, loss, damage, or destruction of information.

Luware AG's current ISO 9001 certification is provided to customers upon request via the responsible sales representative.

8.3.4 STAR Registry

To further enable customers to get a transparent insight into Luware's security measures, Luware has conducted a **self-assessment** and published the relevant information in the Security, Trust, Assurance, and Risk Register.

The register is based on the **CSA Cloud Controls Matrix** which is a cybersecurity control framework for cloud computing. It consists of 197 control objectives that are structured in 17 domains covering key aspects of cloud technology.

9 Appendix

9.1 Data Types - Processing, Erasure and Retention

Data Type	Processing Details	Erasure	Retention
Address Books	Customers can add additional address books to the Attendant Console. Address books contain address book entries with fields for storing contact details such as phone number(s), UPN and external ID. Customers are solely responsible for the correctness, accuracy and lawfulness of this information.	Customers can add, modify and delete the data at any time.	Customer subscription duration plus 30 days
Aggregated Reporting Data	The data combines call detail records, caller information, user time in state if enabled, call treatment and call journey details in aggregated views.	See Call Detail Records, Voicemail Records and User Details.	max. 24 month
Application Logs	Temporary storage of internal application logs to help support engineers troubleshoot the performance and operation of application components.	Can't be erased.	30 days
Attendant Console Log	The Attendant Console Log files are stored locally (per user). They can be erased by the user or will be automatically removed after 120 days.	Can be deleted by the user.	max. 120 days
Audit Trail	Audit trail stores data whenever a change in the configuration is performed. Only Administrator has access to the list, and nobody else can change or delete records. The following information is stored: • Tenant • Office 365 ID of the User	Audit Trail logs all changes made by a user. The action, the date incl. time, name and UPN of the user are recorded. In addition, it records which elements were changed, what the old value was and what the new value of the element is after the save operation.	max. 24 month

Data Type	Processing Details	Erasure	Retention
	• Date/Time of the change • Information of “What has been changed”		
Call Detail Records	Every call which is routed via the Luware Nimbus platform creates a Call Detail Record in the backend database containing the following data: • Caller’s phone number or SIP address • Start/End Time of the call • Routing Decisions • User(s) who answered the call • Voice messages left from a caller on a Luware Nimbus service	For consistent reporting, Call Detail Records cannot be erased, but can be fully anonymized.	max. 24 month
Configuration Data	Customer configuration data of the Nimbus system.	Can't be erased. Configuration data is vital for the correctness of the services provided.	Customer subscription duration plus 30 days
Conversation Context	The Conversation Context allows to add additional information to the caller phone number (e.g. name of the caller). If Information is added e.g. from an external CRM system, it is be stored with the Conversation Context. If Custom Context Parameter is used to display customer information, this information is stored in the Conversation Context. Customers can disable the storage of Conversation Context information within the service configuration. Customers are solely responsible for the correctness, accuracy and lawfulness of this information.	This Conversation Context contains all necessary information which is presented to the agent when a call comes in or is accepted. A toggle on service level enables the customer to decide if they want to store the Conversation Context for 30 days.	Max. 30 days

Data Type	Processing Details	Erasure	Retention
EMail	Incoming EMail will be displayed in the My Service Session page and can be replied to on that page. After the task is terminated, the local data is deleted and only the content from Exchange Online is displayed.	The whole EMail body is presented within Luware Nimbus. The Agent can reply to and send the EMail within Luware Nimbus. After termination of the task, the data is deleted.	Deleted in Luware Nimbus after the task is terminated
Event Logs	Azure Event Logs on the Luware tenant containing user Login attempts.	Can't be erased.	12 months
Transcription data	If the customer decides to use transcription, the whole transcription of a user session is stored. There are several options, which can be configured by the customer. The chosen configuration has an impact on how long the data is stored within Luware Nimbus.	Depending on the Store Conversation Context settings, Transcription will be deleted after 1 hour or after 30 days.	Depending on the chosen configuration up to 30 days
Transcription – Live Caption	Is available only during the call (My Service Session Page) and deleted directly after the user session is terminated.	If Transcription – Live Caption is enabled, the data is deleted after the user session is terminated.	Immediately deleted after termination of a session
Transcription	If the Customer has enabled Store Conversation context for 30 days, transcription is available for 30 days. If this function is disabled, the transcription is offered as a download via Power Automate within one hour of termination of a call and deleted thereafter.	If Store Conversation Context is enabled, data is stored for 30 days, otherwise it is deleted after one hour of termination of the call.	1 h – 30 days dependent on Customer configuration
Transfer History	The history of transfer targets per caller ID is stored in the Attendant Console. Dependent on the call type, this can either be:	The storage of transfers and their targets is essential for reporting. Transfer Targets can be anonymized.	max. 24 month

Data Type	Processing Details	Erasure	Retention
	• Office 365 ID of the transfer target • SIP-address of the transfer target • Phone number of the transfer target		
User Details	For every user that is created in the Luware Nimbus platform the following data is stored in the backend database: • Firstname • Lastname • DisplayName • E-Mail address • UPN / SAM account name	The storage of user details is essential for the correct operation of the system. User details can only be removed from the system by deleting the user, which means that the subject will lose access to the system and reporting data linked to those users will be anonymized.	24 months
User States	To be able to add the user states into historical reporting, the following data is stored in the backend database: • O365 ID of the Office 365 User • Responsibility Profile ID (the user set) • Not Available Reasons ID • Start / End in state as date time • UserState Type (like Offline, Off Duty, Selectable)	If enabled on the tenant, Luware stores the availability status of the user as well as the time in state.	max. 24 month
User Feedback (NPS)	Within the portal we give users the option to provide us with feedback on the solution.	If enabled on the tenant, Luware will store the feedback to deliver a high quality service to customers. The data will be deleted after the evaluation has been performed.	max. 12 month
Voicemail Records	As part of Call Detail Records these are voice messages left from a caller on a Luware Nimbus service.	For consistent reporting, Call Detail Records cannot be erased, but can be fully anonymized.	max. 24 month

9.2 Permissions

In Azure there are two types of permissions:

- **Delegated permissions** are used in the delegated access scenario. These are permissions that allow the application to act on a user's behalf. In this access scenario, a user has signed into a client application. The client application accesses the resource on behalf of the user. Delegated access requires delegated permissions. Both the client and the user must be authorized separately to make the request.

- **Application permissions** are used in the app-only access scenario. These are permissions that allow an application to act on its own behalf. In this access scenario, the application acts on its own with no user signed in. Application access is used in scenarios such as automation and backup.

For more information about these two types of permissions, you can refer to this overview.

Luware Nimbus requires rights within the MS Graph API for basic functions such as call distribution, displaying, and using presence information, but also for displaying caller information. These permissions are only used in connection with Luware Nimbus calls and chats. Without these permissions, the Luware Nimbus Contact Center does not operate.

A detailed description of the Microsoft Application Permissions can be found on the Graph permission reference website as well as on the Azure AD API permission description website.

Calls.*-Permissions: Microsoft Teams acts as the host application for Luware Nimbus. When a call comes into Teams that is destined for Luware Nimbus, Teams invites the Luware Nimbus calling bot to join and control the call. Calls.*-Permissions are used by the Luware Nimbus Calling Bot application and are required to be able to participate in and control calls. Microsoft does not support delegated permissions or scoping for this area.

In any case, the use of the application permissions follows the **principle of least privilege** and is controlled within Luware Nimbus by additional **RBAC** settings – so e.g., only calls intended for Luware Nimbus related teams can be handled by Luware Nimbus users.

A detailed description of all permissions by products can be found in our Knowledge Base.

9.2.1 Application Permission for Email

With the release of Email routing, Luware has introduced additional Application permissions, which are necessary to access mailboxes in Exchange online:

- EMAIL.READWRITE

- EMAIL.SEND

As those permissions are set for the whole customer tenant, we have released the Restrict Access to Mailboxes white paper, demonstrating how to use an Application Restriction policy to limit the access of the Nimbus Application to selected Mailboxes.

9.2.2 Application Permission for Presence

Microsoft has introduced a new way for third-party applications to track user presence with Microsoft Teams. The new feature requires the application to have the

- Presence.Read.All

permission granted on application level. This allows the application to access the presence status of any user in the organization, without relying on the federation or guest accounts.

9.3 Additional Customer Data

There are 2 ways in which additional customer information can enter Luware Nimbus:

- If custom parameters are used for Conversation Context, in the context of or within workflows
- if the following AI features are used:
  - transcription (including live captions),
  - summarization,
  - intend analysis,
  - keyword extraction or
  - Azure AI Service.

If the option to store the Conversation Context for 30 days is enabled in any service, which uses one of those features, the data from the external system and/or the results from the AI functionality are stored within Luware Nimbus for 30 days.

Therefore, customers who use these features are providing additional data to Luware Nimbus, which will be processed and stored. Customers are solely responsible for the correctness, accuracy, and lawfulness of information they put in or store in their Luware Nimbus tenant.

9.3.1 Custom Parameters

Luware Nimbus allows the integration of external applications, e.g. via Power Automate, and then display or save information from these systems in Luware Nimbus. Custom parameters are normally used to transfer this information from other systems. These can be filled with the additional data using Power Automate. If the "Save call context for 30 days" option is activated for the respective service, these custom parameters are also stored within Nimbus for 30 days.

9.3.2 Transcription and Live Caption

Transcription is the process of converting speech to text using artificial intelligence. Luware Nimbus can transcribe audio from phone calls using the Azure Speech Recognizer, which is provided by the customer. There are two different types of transcription:

- Live Caption is generated during the ongoing call. The speech recognizer has less context and therefore the transcription can be less accurate.
- Transcription is generated after the call has been terminated. The speech recognizer has the whole text with all the context and therefore the transcription tends to be more accurate.

Live Caption and Transcription are shown to the user on the My Session page. A Power Automate workflow is triggered and can be used to fetch the transcription content after the call.
Therefore, transcription is stored temporarily in Luware Nimbus - even **if the "Store Conversation Context" flag is not activated for the relevant service** - until the data is picked up via Power Automate. In any case, the transcription is not stored longer than 1 hour within Luware Nimbus.

9.4 Links

Description	Link
Access Restriction Policy (Exchange Online)	Exchange Access Restriction Whitepaper
Azure Physical Security	Physical security of Azure data centers - Microsoft Azure | Microsoft Learn
Cloud Security Alliance	https://cloudsecurityalliance.org/star/registry/luware-ag/services/luware-nimbus/
Conditional Access	What is Conditional Access in Microsoft Entra ID? - Microsoft Entra | Microsoft Learn
Luware Privacy Policy	Privacy Policy | Luware
Luware SaaS Status Page	https://status.luware.cloud
Luware Status and Maintenance Page	Status page
Manage Resources	Resources (luware.com)
Microsoft Azure Well-Architected Framework	Microsoft Azure Well-Architected Framework - Azure Well-Architected Framework | Microsoft Learn
Microsoft Cloud Security Benchmark 1	Overview of the Microsoft cloud security benchmark | Microsoft Learn
Microsoft Cloud Security Framework	https://learn.microsoft.com/en-us/security/benchmark/azure/overview

Description	Link
Microsoft Data center security Overview	Data center security overview - Microsoft Service Assurance | Microsoft Learn
Microsoft Graph Permission Reference	Microsoft Graph permissions reference - Microsoft Graph | Microsoft Learn
Microsoft people security	Personnel management overview - Microsoft Service Assurance | Microsoft Learn
Microsoft permission and consent overview	Overview of permissions and consent in the Microsoft identity platform - Microsoft Entra | Microsoft Learn
OAUTH2 authentication with Azure Active Directory	OAUTH 2.0 authentication with Azure Active Directory - Microsoft Entra | Microsoft Learn
Power BI	https://help.luware.com/nimbus/latest/usage-of-nimbus/power-bi
Service SettingsService Settings	https://help.luware.com/nimbus/latest/usage-of-nimbus/nimbus-teams-tab/service-settings
Services	https://help.luware.com/nimbus/latest/administration/service-administration
Shared Responsibility.	https://azure.microsoft.com/en-gb/resources/shared-responsibility-for-cloud-computing/
STAR Registry Listing for Luware Nimbus	STAR Registry Listing for Luware Nimbus | CSA (cloudsecurityalliance.org)
User Administration	https://help.luware.com/nimbus/latest/administration/user-administration

9.5 Glossary

Term	Description
Access	Access refers to the ability to use computing resources such as applications, servers (physical servers and virtual servers), data storage, development tools, networking capabilities, and more that are hosted at a remote data center managed by a cloud services provider. Cloud computing is on-demand access via the internet to computing resources.
Application Service Accounts	Application service accounts are user accounts that are created for applications or services to use when accessing other systems or services.
Authentication	Authentication is the process of verifying someone's or something's identity. Authentication usually takes place by

Term	Description
	checking a password, a hardware token, or some other piece of information that proves identity
Conditional Access	Conditional Access is a policy-based service that allows you to control access to your organization's applications and resources
Generic User Accounts	A generic user account is a user account that is shared by multiple users. It is often used for system-level tasks that do not require personalization or individual user accounts.
Graph Communications API (Microsoft Graph)	A set of APIs that enable developers to create applications that can make calls, join meetings, or send chat messages in Teams using the Microsoft Graph platform.
Multi-factor authentication (MFA)	Multi-factor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.
Organization	Company using Luware Nimbus
Partner Administrator	Users listed in the partner administrator Microsoft Entra group. A partner administrator is the tenant administrator for all tenants associated with a partner.
Recovery Point Objective	Recovery Point Objective refers to the maximum amount of data that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organization 1. In other words, it is the time period between two data backups
Recovery Time Objective	Recovery Time Objective refers to the maximum amount of time that an organization can tolerate for systems and applications to be unavailable after a disaster or disruption. It is the time period within which an IT resource must fully recover from a disruptive event. The RTO is an essential component of a Disaster Recovery Plan (DRP) and is part of a Business Impact Analysis. The RTO is usually determined by the criticality of the application, with more critical applications requiring shorter RTOs than those that are less critical.
Service Administrator/ Team Owner	Automatically synchronized with Microsoft Teams channel roles. Automatically granted permissions to fully manage each Luware Nimbus service. No manual assignment required
Services	Luware Nimbus distinguishes between two primary types of services: User Assignment and Group Assignment.

Term	Description
	Additionally, there are two distinct methods for integrating Luware Nimbus within Teams: Teams-based integration and skill-based integration.
Shared Responsibility	The Shared Responsibility Model is a framework that outlines the responsibilities of cloud service providers and customers for securing every aspect of the cloud environment. This includes hardware, infrastructure, endpoints, data, configurations, settings, operating system (OS), network controls and access rights. It describes the responsibility of each participant of the scenario.
Software-as-a-Service (SaaS)	SaaS is a software licensing model that allows users to access programs via the Internet on a subscription basis using external servers.
Tenant Administrator	The user is listed in the tenant administrator's Microsoft Entra group. The tenant administrator has full configuration control within the Luware Nimbus tenant.
User	Person using Microsoft Teams within an organization

/end

solutions@luware.com
+41 58 404 28 00
www.luware.com