Security Overview

Nuvolex is an ISV that develops products to optimize provisioning and ongoing administration of public cloud services. A major consideration of cloud services administration is security and privacy. Security can take on many definitions when it comes to public cloud services; ranging from application security, infrastructure and data security as well as data privacy and trust.

Every process step in our application development and delivery is concerned with maintaining the utmost secure practices and industry standard procedures - from building the Nuvolex platform through maintenance and support. Our goal is to produce the IT industry's best public cloud management platform, employing secure coding standards, and delivered through a reliable and protected environment to ensure customer data is kept private and secure.

Commitment to Privacy

Nuvolex treats your data with the privacy and respect that you would expect from your own IT staff. We guarantee that your data is secure and kept private. Nuvolex generates its revenue solely from selling platform licenses. We do not sell customer data to any third party vendors. The only people with access to your data are the Nuvolex administrators that have been given access rights to view and manage your data. All imported data services (AD, Azure AD, and Office 365) are stored in an Azure Database that is encrypted at rest as well as in transit, to further data security and privacy. Nuvolex employees and suppliers will not have access to your data unless explicit requests are granted by you.

Responsive to Threats

Nuvolex stays up to date on the latest changes to the constantly evolving global threat landscape. This includes monthly patches to our virtual machines and the services running on top of them. Nuvolex runs a quarterly vulnerability scan using industry standard tools such as Nessus, to confirm that no known security issues exist. Before any new changes are committed to our code repository, a static analysis is performed to expose any vulnerabilities. If any vulnerabilities are found in the code, we log the vulnerability, resolve it and immediately run the static analysis again to verify the code fix. Once the code base comes back with a clean bill of health, the new code is committed to our repository to be built into a new version of the Nuvolex application, and only then, released to production.

Data Breach Reporting

The Nuvolex environment is consistently monitored for threats and the possibility of intrusions. In the event of a security breach, we are alerted through a combination of intrusion detection and log analysis systems. When a breach is verified, we isolate the virtual machine and force all connections to the VM to close. We then take the needed measures to prevent any follow up breaches. We then audit our systems to ensure that the threat has been eliminated and also measure the extent of the threat. Following this process, we can determine the impact of the threat to see if data has been compromised. Based on our analysis we will inform compromised customers of the breach. In the event where personally identifiable information has been compromised by a threat, Nuvolex will report the breach directly to the customer within 72 hours. We will outline how the threat occurred, its behavior, and the scope of compromised data with potential impacts to the customer's user base and organization. Doing this ensures that customers are aware of all threats that impact their users and organization. We will not publish any press of a breach unless legally required to do so. Customers will be notified if Nuvolex will be putting out a breach related press release.

Nuvolex's Role in Data Protection

In the context of data protection and privacy, Nuvolex plays the role of the Data Processor which processes Customer Data that contains Personal Data relating to Data Subjects. The Customer who is using Nuvolex to manage their public cloud services and users is the Data Controller, and has the responsibility for ensuring the accuracy, quality and legality of their Personal Data and the means by which Personal Data is collected. As a Data Processor, Nuvolex, and its suppliers shall keep Personal Data confidential and secure using industry standard best practices that comply with data protection guidelines.

Data Protection Officer

Nuvolex has appointed a Data Protection Officer (DPO) which is responsible for overseeing the Nuvolex Data Protection Strategy and implementation to ensure compliance with legal and customer requirements. The DPO is also responsible for educating the company and its employees on importance of compliance and conducting regular security audits. The Nuvolex DPO will serve as the point of contact for all data protection issues, inquires and data requests. The Nuvolex DPO can be reached at privacy@nuvolex.com.

Application Security

Secure Coding Practices

Security is a priority throughout the development cycle when adding any new functionality to the Nuvolex platform, or when making a change to existing functionality on the platform. For all newly developed code, security starts at the Product Requirements stage in order to address potential security concerns. The product development team builds the required functionality while addressing any potential security concerns. Then the development team performs a code review to validate that no defects or logic flaws exist. Lastly, the QA stage not only tests the application to validate the functionality works as expected, but also identifies areas of potential risk for exploitation and tests to see the outcomes of these identified areas. Once all issues have been resolved, the application is put through a dynamic fuzzing scan and a static analysis to further test the integrity of the code.

Application Sessions

Sessions are generated once a user is authenticated and signed in to the Nuvolex platform. The session is permanently disposed (made invalid) once the user has logged out or after one hour of idle time. Session IDs are a randomly generated hexadecimal number that is unique to each user authentication. This will make it so that the same session ID can only be used once. If there is an attempt to use the same session ID again, the session ID will be made invalid to prevent replay attacks. Only one valid session is allowed per user login at a time, so that the same IT administrator using the same credentials cannot be logged in from two different locations. This is achieved by utilizing a session fixation protection configuration in our backend security framework.

All actions on the platform must be made using a REST call. REST calls can only be made using a valid session gained after a successful user authentication. Any application REST calls to retrieve data execute an action must come from a valid browser session which is created at the time of a successful authentication into the Nuvolex platform. If a call is being made without a valid session, the call is denied.

Cookies

When a user logs in, a session cookie is created that stores the valid session ID assigned to the logged in Nuvolex Administrator. This cookie expires or is removed when the session is closed, or times out.

The UI saves two cookies in the browser the first of which consists of storing the last accessed tenant, and another cookie that saves the name of that tenant. These two cookies are used to support user experience by preselecting tenants for the Nuvolex Administrator upon login.

Role Based Access Controls

Nuvolex Role Based Access Control features provide the ability to easily set very granular levels of administrator access. Nuvolex Administrators can be assigned access to a strict set of users and actions an IT administrator is allowed perform on the tenants being managed. As a result, you can control who in your organization has access to data and what level of access they have.

Access Controls for each Nuvolex Administrator or Administrator Group is split up into 4 categories:

- **Authorized Actions**
  - The ability to define a very granular levels of tenant access for each Nuvolex administrator or administrator Group. Authorized actions can be very broad or heavily restricted, depending on the responsibilities of each administrator or administrator group using the Nuvolex platform. One example of controlled access rights would be whether or not an administrator is allowed manage various user groups or assign Office 365 licenses.
- **Authorized Tenants**
  - The ability to assign a Nuvolex administrator or administrator group access rights to one or many tenants. When a Nuvolex administrator logs onto the platform, they will only have visibility and access to the tenants that they have been given access rights to. Tenant assignment on the platform uses a "default deny" model, so you must explicitly enable specific tenant access for each Nuvolex administrator.
- **Authorized Domains**
  - The ability to define the specific AD Domains that a Nuvolex administrator or administrator group has access to. If access control is required at the AD Domain level, this is easily accomplished with the Nuvolex platform by selecting one or many AD domains that you want to grant a Nuvolex administrator access to.
- **Authorized Organizational Units**
  - The ability to assign a Nuvolex administrator or administrator group to one or many organizational units (OUs) inside of tenant. When a Nuvolex administrator logs into the platform, they will only see the users that are in the specific OUs that they have been given access rights to. OU assignment uses a "default deny" model, so you must explicitly allow each OU that the Nuvolex administrator has access to. OUs on the Nuvolex platform can be imported from Active Directory or can be created in the Nuvolex platform.

Data Collection

The Nuvolex platform will collect various types of data to support the extensive management functionality and to provide an always available and responsive management experience. Data is collected from a variety of workload sources such as Active Directory, Azure AD, Exchange Online, SharePoint Online and many other Microsoft services. Data is also collected directly from each Nuvolex administrator. The specific data sets that are collected are necessary to enable operation of the Nuvolex platform. All data that is imported and synchronized from Microsoft 365 services, Azure AD, Active Directory or directly from users of the Nuvolex application is needed in order to provide an IT Administrator the ability to effectively manage all assigned tenants and users. At no time does the Nuvolex platform store or make changes to data that exist outside of the defined scope of the platform. All tenant data is stored using the methods mentioned in the ***Data Security*** section.

Tenant Data

Tenant Data is defined as top level information and configurations on an individual organization that has onboarded any Microsoft 365 services (Exchange, Teams, OneDrive etc.) and/or Active Directory data into the Nuvolex Platform. Users of the Nuvolex platform can onboard an unlimited number of Microsoft 365 tenants into their Nuvolex account, thereby creating several tenant level data collections. The following information is captured by the Nuvolex platform:

- **Tenant Name**
  Used to identify the specific Microsoft 365 tenant being managed by an administrator on the Nuvolex platform.

- **Microsoft 365 Global IT Administrator Credentials**
  The Nuvolex platform uses the Microsoft 365 Global Administrator Credentials to authenticate to your tenant using PowerShell in order to access data and push updates to Exchange Online, Skype for Business, Azure AD. Global Administrator Credentials are always encrypted using specific keys and will never be visible to users on the Nuvolex platform or to the Nuvolex team.

- **Tenant Address**
  Used as a part of the Nuvolex tenant record for customer billing purposes.

- **Tenant Phone Number**
  Used as a part of the Nuvolex tenant record for customer communication.

- **Subscribed Microsoft 365 License SKUs**
  Storing licensing information allows us to deliver an optimized user experience when managing tenant licenses. We collect license data for the subscribed SKUs of each tenant being managed on the platform, as well as the available and assigned licenses for each Microsoft 365 user.

- **Registered Domains for Microsoft 365 Tenants**
  Keeping a list of valid domains enables the Nuvolex platform the ability to quickly reference if an email address is unique as well as providing a more thorough user management experience by forcing proper domain usage based on the registered tenant domains.

- **DirSync Status**
  Knowing the DirSync status of a tenant will impact the way tenant data is handled. There are several limitations on functionality if a tenant is DirSync enabled. The functionality of the Nuvolex platform is modified to comply with these limitations based on a tenant's DirSync status.

- **Company Contact Details**
  The Nuvolex platform stores the company contact configuration for an Microsoft 365 tenant. These contact details are displayed to the Nuvolex administrator and can be modified. The contact details are limited to the following: Marketing Notification Emails, Configured Privacy Policy, Security Compliance Notification Emails, Security Compliance Notification Phones, Technical Notification Emails.

- **Self Service Password Reset Settings**

The Nuvolex platform stores the Self Service Password configuration for a Microsoft 365 tenant. The configurations can be viewed and modified.

- **Groups creation settings**
  The Nuvolex platform stores the group creation configuration for a Microsoft 365 tenant. The configurations can be viewed and modified.

- **Line of business app creation settings**
  The Nuvolex platform stores the line of business app creation configuration for a Microsoft 365 tenant. The configurations can be viewed and modified.

- **Users consent to app permissions settings**
  The Nuvolex platform stores the user consent enablement configuration for a Microsoft 365 tenant. The configurations can be viewed and modified.

- **Default usage location**
  The Nuvolex platform stores the default usage location for a Microsoft 365 tenant. The configurations can be viewed and modified.

- **Password Expiration settings**
  The Nuvolex platform stores the password expiration configuration for a Microsoft 365 tenant including the number days before passwords expire and the number of days before a user is notified about expiration. The configurations can be viewed and modified.

- **Workload auditing settings**
  The Nuvolex platform stores the workload auditing configuration for Exchange, Intune, SharePoint, OneDrive services for a Microsoft 365 tenant. The configurations can be viewed and modified.

- **SharePoint Default Sharing Link Type**
  The Nuvolex platform stores the default sharing link configuration for SharePoint services in a Microsoft 365 tenant. The configurations can be viewed and modified.

- **Infected file downloads from SharePoint configuration**
  The Nuvolex platform stores the configuration for how to handle infected files in SharePoint for a Microsoft 365 tenant. The configurations can be viewed and modified.

- **Set Default OneDrive storage quota**
  The Nuvolex platform stores the default OneDrive storage quota for OneDrive services in a Microsoft 365 tenant. The configurations can be viewed and modified.

- **Allowed/blocked domains for sharing**
  The Nuvolex platform stores the allowed and blocked domain configurations for SharePoint and OneDrive services in a Microsoft 365 tenant. The configurations can be viewed and modified.

- **External Sharing permissions**
  The Nuvolex platform stores the external sharing permissions configuration for SharePoint and OneDrive services in a Microsoft 365 tenant. The configurations can be viewed and modified.

User Data

User Data is defined as data sets tied to individual users from each onboarded tenant from Microsoft 365 and Active Directory. User Data contains very specific information on end users, but this information is limited to only the data required by Nuvolex administrators to effectively manage identities for Microsoft 365, Azure AD and Active Directory users on the Nuvolex platform. User Data is initially imported from Azure AD, Microsoft 365 and Active Directory and then synchronized with any changes made to user data in either Microsoft 365, Azure AD and Active Directory. User Data can also be specific to the services that are consumed by each user, such as a user's Exchange Online mailbox configurations, SharePoint site access rights and Group memberships. At any time, a Nuvolex administrator is able to make changes to any user data that the administrator has been permitted access to.

The following User Data is captured by the Nuvolex platform and made readily available for the Nuvolex administrator to manage as well as to improve usability and system responsiveness:

- **First Name, Last Name**
  Used for user object identification.

- **Display Name**
  Used for user object identification.

- **Phone Number**

  A user's office and mobile number are added as a part of a user record.

- **Department**
  Added as a part of the user record.

- **Address**
  Added as a part of the user record.

- **Job Title**
  Added as a part of the user record.

- **Microsoft 365 Service Usage Location**
  Added as a part of the user record.

- **Group Memberships**
  Added as a part of the user record, used to support Group management functionality.

- **User Principal Name**
  Added as a part of the user record, used for user identification and referenced to ensure unique email addresses are used throughout the tenant.

- **Primary SMTP Email Address**
  Added as a part of the user record, referenced to ensure unique email addresses are used throughout the tenant.

- **User Mailbox Aliases**
  Added as a part of the user record, referenced to ensure unique email addresses are used throughout the tenant.

- **Account Status**
  Added as a part of the user record.

- **Immutable ID**
  Used for user object identification when applying changes to users in Microsoft 365 services to ensure the accuracy of the changes being made.

- **User Source Data**
  Used to determine the source of a user's identity object such as Azure AD or AD.

Group Data

- **Group Name**
  Used for Group identification during Group management scenarios.

- **Group Display Name**
  Used for Group identification during Group management scenarios.

- **Group Email Address**
  Used for Distribution and Office 365 Group identification and referenced to ensure unique email addresses are used throughout the tenant.

- **Group Alias**
  Used during Distribution Group management scenarios due to Group Aliases being a required attribute for Microsoft 365 services.

- **Group Options**
  Hide from Global Address List and Require Sender Authentication are both used during Distribution Group management scenarios.

- **Group Owner**
  Used during Group management scenarios due to Group Owners being a required attribute for Microsoft 365 services.

- **Group Membership**
  Used during Group management scenarios. Group membership lists are stored to provide quick and accurate information on which users are part of a specific Group vs users who are not. This data is also used to provide a list of eligible users who can be added to other Groups.

- **Security Identifier (SID)**
  Used for unique group identification when applying changes to Groups in Microsoft 365.

Nuvolex Administrator Data

- **First Name and Last Name**
  Used as information in the administrator user record for identification and general usage.

- **Email Address**
  The Nuvolex administrator email address is their username. Used to ensure that administrator accounts are each unique and also for sign-in purposes.

- **Password**
  Used during the sign-in process to authenticate a Nuvolex administrator. Stored and encrypted in the Nuvolex LDAP system which is responsible for authentication processes.

- **IT Administrator Privileges**
  - Tenant Access, OU Access, AD Domain Access, Functionality Access

  In order to provide accurate Role Based Access Control capabilities on the Nuvolex platform, assigned privileges need to be stored in the Nuvolex database and referenced during login to deliver each Nuvolex administrator the proper tenants, users and management functionality.

- **Azure AD User Principal Name**
  An administrator's user principal name (UPN) is used for Azure AD SSO operations. A Nuvolex administrator may sign into the Nuvolex platform using Azure AD SSO which provides the Nuvolex application with a set of claims that contains the authenticated user's UPN. The UPN is used to retrieve the administrator's authorization on the Nuvolex platform.

Data We Do Not Collect

The Nuvolex platform is focused on data sets that relate to user identity objects and the various attributes that are tied to a user identity object. Additional data sets collected are resources that end users utilize in cloud services such as Office 365 mailboxes, SharePoint sites, and Teams. Nuvolex does not obtain sensitive user data such as end user passwords, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. At no time will the Nuvolex platform support any of the above data sets since they are not related to the primary use of the Nuvolex platform service.

Data Collection Scope Monitoring

The Nuvolex platform is designed to only query, import and make changes to the data sets listed in the above sections. The Nuvolex platform does not move beyond these specified data sets since that information is not required to perform the management functions of the Nuvolex platform. The goal of the Nuvolex platform is to manage user identities and cloud resources, therefore the required data set to accomplish this goal is concise and strict controls on data handling and data importing are always enforced. The Nuvolex team frequently audits the data sets that are imported and handled from cloud services to validate that the supported data set has not changed and that the data we consume is consistent.

Nuvolex DEV & QA Environments

The Nuvolex DEV and QA environments run independently and are completely isolated from the Nuvolex production environment. DEV and QA resources are deployed and run in a different Azure tenant than the production environment to provide a additional level of isolation between the Nuvolex production environment and the DEV & QA environments. Because of this isolation, customer data that is hosted in the Nuvolex production environment is unable to be used by DEV and QA environments. At no time will customer data be used during the DEV and QA cycle.

Changes to Data Collections

The data set that is supported and imported by the Nuvolex platform seldom changes, but is continually expanding as the Nuvolex expands its workload and functional management capabilities. If the scope of the Nuvolex required data set that that is imported and stored by the Nuvolex platform changes, we will provide updates to our Security White Paper. Due to the nature of the updates, customers may need to give Nuvolex explicit consent to process the new set of data. It is unlikely this will be case, however we are continuously monitoring and assessing the impact of the data set we support today, and the set of data required for future functionality add.

Data Security

The Nuvolex platform database is hosted on Azure. All customer data is encrypted end to end using a combination of AES-256 keys that are designated for specific functions to ensure that data is kept secure and private. The database has been configured to use TLS when communicating with the front-end web application server using a dedicated RSA 2048-bit key pair that enables 256-bit TLS data “in transit” encryption.

Encryption at rest has been enabled for the Nuvolex Database so that all customer data is securely stored and kept private. The Nuvolex Database uses storage encryption for data at-rest. Data, including backups, are encrypted on disk. The Nuvolex Database uses AES 256-bit cipher that is included in Azure storage encryption and the keys are system managed.

Database backups maintain the same level of encryption (AES-256) that is used in the running database so that all data remains secured regardless of its location. Our database encryption strategy not only keeps customer data safe from malicious entities, but it also helps promote data privacy. Data is decrypted once the platform handles and passes the data into the UI which can only be seen by a user logged into a specific tenant with valid permissions.

The Nuvolex platform is deployed and runs on a purely US based Azure infrastructure that encompasses compute, DB, and networking services. All Nuvolex platform data is stored and accessed through the Nuvolex Azure environment. At no time will Nuvolex application data be stored physically in any on premise locations outside of the US based Azure resources.

Infrastructure Security

The entire Nuvolex infrastructure is hosted in Microsoft Azure with strict access policies for all of the production virtual machines. Microsoft Azure is compliant with ISO 27001, HIPAA, DISA, FISMA, PCI, FIPS 104-2, SOX, plus more which can be referenced here.

The Nuvolex VMs are placed into a private local network isolated from other environments and tenants. All hosts communicate locally allowing for a very limited amount of ports to be open to the public internet. The only ports we have opened to the public internet are HTTP, HTTPS, and VPN ports.

Management access for all host VMs is done exclusively through an Azure with a site-to-site VPN that is connected to the Nuvolex HQ network. There is no ability to obtain remote access to any of our VM over the public internet. Each host VM is joined to an Active Directory Domain (hosted in Azure), so that authentication into each host VM is done securely from a central authentication authority, enabling enhanced authentication control and auditing. Local accounts on all host VMs have been disabled forcing host authentication to be done with a domain user account.

All the component services are configured using the security best practices and industry standards to ensure that all exploitable functions for each component service is secured. Continuous patching is performed to stay in front of all the discovered exploitable functions of each of the component services that run the Nuvolex platform.

The Nuvolex platform is accessed exclusively over TLS. The certificate used identifies the origin and name of the server and encrypts all data that is sent between the web browser and the web application server and is SHA-256 certificate signed using a 2048 RSA by GoDaddy Certificate Authority.

The Nuvolex platform sits behind the web application firewall which inspects all incoming traffic for malicious or unauthorized behavior such as cross site scripting, SQL injections, logic bombs, DDOS attacks as well as other common web application exploits. The WAF is able to recognize these behaviors and deter any attempts from occurring. All web traffic to the Nuvolex web application must pass through the web application firewall to gain access. There is no ability to connect to the front-end web host directly over the public internet.

Key Management

Nuvolex uses a number of keys and key pairs and encryption standards to securely store and interact with data. To ensure consistency and security we have implemented an industry standard key management system to enforce key management life cycle for all keys that are used throughout the Nuvolex environment.

Keys are generated, distributed, stored and rotated from a centralized system inside of our Azure environment. Keys are generated and then confirmed for a specific use such as data at rest encryption or for a VPN gateway plus many other critical functions. Keys are rotated yearly, with retired keys being recorded and securely destroyed. All stored keys are encrypted, and the keys remain encrypted in any backups.

Authentication to Servers, Nodes and Infrastructure

All Azure hosted compute endpoints utilize centralized authentication through Azure hosted Active Directory Domain Services. Nuvolex IT staff authenticate to hosts using AD credentials that can be easily audited and controlled. The internal Nuvolex IT Staff administrator credentials expire every 90 days, with password history restrictions.

Disaster Recovery

Nuvolex has developed and continually tests a disaster recovery procedure that will ensure that the Nuvolex service and customer data remains available and accessible. The Nuvolex disaster recovery procedure focuses on service availability and data accessibility. The Nuvolex disaster recovery plan outlines methods in which customer data will never be lost due to system failure, or other means of a service outage. In the cases where a disaster scenario is encountered, the Nuvolex service will be restored within a short timeframe.

Retention Policy

Nuvolex application data is backed up nightly and retained for a maximum of 30 days to ensure data is never lost due to disastrous and destructive conditions. Since the nature of the Nuvolex platform is to sync data from external sources (Microsoft 365, Azure AD etc.) it is not required for Nuvolex to maintain long term records or backups of application data. The Nuvolex retention policy reflects the absolute bare minimum duration for business continuity and data loss prevention activities.

Annual Training

All Nuvolex employees receive yearly security and data handling training to further the implementation and execution of data security and privacy practices. Nuvolex employee yearly training covers recognizing and responding to security threats as well as updates and refreshers for how to identify and how to handle Personally Identifiable Information.

Continuous Security Development

As security systems, processes and applications evolve so does the global threat landscape. Nuvolex continually assesses our security strategy to stay ahead of any potential risks. This is done by keeping current with new security innovations that appear on the market as well as working often with security experts and auditors to further improve our strategy to meet higher tiers of compliance.