Data Protection and Security on the AppNexus Platform

Data Protection and Security on the AppNexus Platform

> For detailed information on how AppNexus is working within the GDPR and ePrivacy framework with regard to information security, go to our GDPR space and review the Information Security page. (*Note: you will need your client wiki login to access the page.*)

Disclaimer

This document reflects current practice as of the Effective Date of this document. The processes, controls, and safeguards described are subject to modification as circumstances change, but will always be reasonable as determined by AppNexus based on consideration of risk and generally accepted industry practice for the types of data and systems involved. AppNexus will endeavor to update this document as changes are made. You may always ask your AppNexus representative for the latest version.

Overview

AppNexus is committed to protecting personal, private, confidential, and sensitive data and the systems used to process, store, or transport such data. This is includes, but is not limited to, customer data, employee data, and company, vendor, and partner proprietary data. To that end, this document outlines the measures employed by AppNexus towards that commitment.

Safeguards fall into the following areas:

1. Physical Access
2. Electronic Access
3. Credentials and Account Controls
4. Data and Application Access Controls
5. Intended Data Use and Handling
6. Technical Safeguards
7. Policies and Awareness

Physical Access

The following measures have been taken to ensure that unauthorized persons cannot physically access AppNexus data or data processing equipment.

Physical assets (servers, switches, data storage devices, etc.) used for storing or processing personal, private, and sensitive data are located in commercial Tier 4 data centers owned and operated by industry leading firms who certify through external audit to the SSAE 16 standard. This standard ensures that a high and consistent degree of security, process, and controls are employed to control physical access to AppNexus assets. Safeguards typically include, but are not limited to:

- Video surveillance (outside facilities and in-doors)
- Two-factor security for granting access (e.g. transponder card and pin, biometric scan and pin) with logging
- 24 hour guard services with linked alarm system
- Separate physical security zones for office areas, data center equipment areas, and customer work areas, etc
- Separation of duties, with checks and balances, to ensure compliant execution

Physical access to AppNexus data processing equipment is only granted to authorized staff. The authorized staff list is reviewed and scrubbed regularly to ensure it is current and appropriate.

Physical access to AppNexus business offices and staff areas is typically controlled and monitored with the following safeguards:

- Video surveillance – (workspaces, corridors, etc.)
- Transponder-card/fob controlled locks on all exterior doors
- Card holder's photo and full name are on transponder-cards
- Credentialed staff receive transponder-cards or equivalent with only door access appropriate for their role

Electronic Access

Access to AppNexus systems requires authentication and authorization with the exception of information that AppNexus intentionally makes

publicly available such as the corporate web site and parts of the customer facing wiki. Communications are usually restricted to encrypted channels with the use encryption increasing and expected to eventually include almost all communications generally excepting only those which cannot utilize encryption without compromising functionality. The sharing of login credentials is strictly prohibited by AppNexus policy. An automated centralized account management system is used to manage most end user credentials with the reach of this system increasing over time and expected to eventually cover almost all if not all systems. Further, the roster of privileged users (e.g. system administrators, database administrators, network administrators) is reviewed regularly by AppNexus TechOps management and the roster adjusted accordingly to ensure it is always current and appropriate.

Credentials and Account Controls

All AppNexus workforce members (employees, contractors, interns, etc.) receive a User Account which uniquely identifies them for access to all AppNexus data and applications. AppNexus mandates that all Users protect their User Account with passwords that conform to AppNexus policy in terms of password length, complexity, expiry, and reuse. Users are prohibited from sharing credentials or compromising passwords by storing them in or on any unprotected medium in clear readable text form.

All role changes, such as promotions, terminations, job changes, department changes, employment status changes, etc., are reflected in User Account access rights as appropriate.

An automated centralized account management system is used to manage most User Accounts with the reach of this system increasing over time and expected to eventually constitute almost all if not all systems. Recertification of users' status and access occurs periodically. Functional team managers participate in this process to ensure accuracy and accountability for correctness of data.

Additional care for Privileged Access and Accounts

Privileged accesses, such as those required by various Administrators to perform certain necessary job functions, are associated with appropriate User Accounts whenever possible to maximize accountability and audibility. When a dedicated privileged User Account is required by an application or system the same guidelines that apply to normal User Accounts as outlined above apply to the dedicated privileged User Account to the greatest extent possible. Dedicated privileged User Accounts are used only for administrative tasks that require administrative privileges; they are not used for convenience and all non-administrative tasks are executed using a normal user account. When an application or system supports multiple dedicated privileged User Accounts then each Administrator has and uses a separate and unique dedicated privileged User Account. Dedicated privileged User Accounts are not shared unless an application or system does not support multiple dedicated privileged User Accounts. All User Accounts which come pre-configured with new hardware and/or software by default are disabled. Only those User Accounts required for the proper operation of an application or system are enabled.

Data and Applications Access Controls

AppNexus Data should be accessed through applications which implement appropriate access controls and limitations whenever possible. Direct access to data is prohibited by policy and prevented to the greatest extent possible through a combination of technical safeguards such as application permissions, network security mechanisms, firewalls, operating system and file system permissions and security mechanisms, and database permissions and security mechanisms. Privileged and direct access to data, for the purposes of authorized system tasks (e.g. application and/or system maintenance, problem remediation), is limited to ONLY to authorized AppNexus Administrators.

Application user-access permissions govern what data can be accessed and what systems functions and data operations a user can perform (e.g. add, change, delete, view). AppNexus uses Role Based Access Controls (RBACs) and the principal of Least Privilege. User access rights are only granted through properly documented and approved processes. To ensure that application access remains appropriate and accurate, access rights for each application and each user are reviewed, corrected, and re-certified on a regular basis by application owners and managers.

Technical Safeguards

Protecting data stored

Personal, private, confidential, and sensitive data including, but not but limited, to customer data, employee data, research and market data, and company, vendor, and partner proprietary data are all considered "protected data". AppNexus reasonably prevents unauthorized access to protected data by employing the following technical safeguards:

Private Networks and Network segmentation: AppNexus places systems and storage devices processing or containing protected data on AppNexus private networks accessible only to authorized users, applications, and devices.
Firewalls / Access Lists / Proxies: AppNexus uses a combination of Firewalls, Access Lists, and Proxy devices to limit access to only authorized user, applications, and devices.
File System, OS, and Database Technology: AppNexus uses a combination of the security and access control features of File Systems, Operating Systems, and Database Systems wherever practically possible, and to limit access to only authorized user, applications, and devices.

Protecting transmitted data

All protected data transferred past the boundaries of AppNexus infrastructure either authenticated and encrypted communication protocols (e.g. SCP, SFTP, SSL) or use internal private networks, point to point external networks, or a combination thereunto wherever practically possible, to protect the data in transit.

Intended Data Use and Handling

Through a combination of application logging, data access logging, business reporting, and employee training and management, AppNexus endeavors to ensures that data is accessed, used, and handled in a manner consistent with all provisions outlined in agreements between AppNexus and customers/partners, and the laws and regulations governing AppNexus business.

Policies, Procedures, Standards, Guidelines and Awareness

AppNexus employees are contractually bound to confidentiality and AppNexus communicates expected behaviors related to data protection and safeguards to its staff.