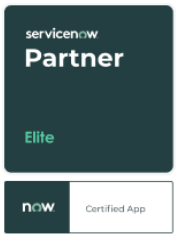

PLATCORE

Service Level Agreement 2023

sales@platcore.com • 1-844-205-7789

PLATCORE INDEX

SaaS Delivery Model

ServiceNow will manage and maintain the required infrastructure (hardware and software) in their secure data centers. ServiceNow's data centers and cloud-based infrastructure are designed to be highly available. All servers and network devices have redundant components and multiple network paths to avoid single points of failure. They deploy instances on a per-customer basis, allowing the multi-instance cloud to scale horizontally to meet each customer's performance needs. Each instance runs its own application logic and database processes. Production application servers are load balanced within each data center. Production database servers are replicated in near-real time to a peer data center within the same geographic region. All customer production data is stored in both data centers and kept in sync using real-time database replication. Both data centers are active at all times, each with the ability to support the combined production load of the pair. In the event of the failure of one or more infrastructure components, service is restored by transferring the operation of customer instances associated with the failed components to the peer data center.

ServiceNow continually tests the scalability of their technology using internal testing tools. They have tested their database scalability using very large datasets (millions of rows) and large transaction volumes. Their largest clients have hundreds of thousands of employees accessing the system every day. ServiceNow monitors and manages capacity from their centralized Network Operation Center and adjusts capacity as necessary. There are no hard limits on storage capacity.

User Interface

There is no client to install to access the LMS. The only requirement is a web browser and an internet/network connection. The ServiceNow Platform supports the latest version or service pack of the following browsers: Firefox and Firefox ESR, Chrome, Safari version 9.1 and up, Microsoft Edge and Internet Explorer version 11 and up (Edge mode is supported). In addition, the LMS can be accessed using either an IOS or Android mobile device using browser technology.

Security

ServiceNow understands that the confidentiality, integrity, and availability of customer data is vital to all organizations, regardless of size. The ServiceNow Platform provides features and services – in a secure, reliable environment – that support COTS implementations, as well as custom applications, and application integrations. ServiceNow provides 24x7 operations and security monitoring to help ensure customer instances are protected and operating as intended. ServiceNow employs a multi-instance architecture delivered via SaaS that is protected by an enhanced, defense-in-depth framework of firewalls, load balancers and intrusion detection systems (IDS). The solution is hosted

within geographically separated, secure data centers. ServiceNow internal security includes access control through Access Control Lists (ACLs), integration with Active Directory/LDAP, authentication and single sign-on, auditing and system logs, communications security, company and domain separation, contextual security, and data encryption and integrity. It also supports highly secure integrations between ServiceNow, customer, and other third-party infrastructures.

Advanced protections isolate customer data from other customer data by leveraging an enterprise-grade cloud architecture and a dedicated database and application set. All ServiceNow data centers maintain industry standard SSAE16/SOC1 Type II attestation or ISO 27001 certifications, which provide third-party verification of the data center controls, security measures and operational processes that supply physical security protection and facilities support for the ServiceNow environment.

ServiceNow achieved the highest level of certification for a wide range of industry standards and industry-specific compliance including SSAE16/SOC1 Type II and ISO 27001, Pharmaceutical industry IQOQ and a government-wide FISMA Moderate certification. All ServiceNow customers receive advanced high availability on production instances including data replication to a geographically separated data center.

User Authentication

To give you the most flexibility, ServiceNow supports several authentication options. This allows you to use several methods within your instance. Your instance supports “native” or local authentication (for example, when user credentials are stored in the instance) and Oauth 2.0 authentication (such as for external client authentication), as well as multi-factor authentication mechanisms. The ServiceNow SAML plugin supports SSO-based authentication through a variety of SAML 2.0-compliant identity providers. This include Active Directory Federation Services (ADFS) as well as third-party identify providers, such as Ping, SecureAuth, SailPoint, Okta, or others that are compliant with the SAML 2.0 standard. If you have already implemented your own SAML-compliant IDP or leverage a third-party service, you can use the same capability for your ServiceNow instance. LDAP authentication enables customers to use their own LDAP-compliant directory services such as Active Directory. A directory needs to be accessible to the relevant ServiceNow instance, as often these are located behind a firewall or other perimeter control. As part of the LDAP integration, passwords are not stored or transferred back to your ServiceNow instance.

You have full control of entitlements granted to each of your end users in a ServiceNow instance. This includes a built-in Role Based Access Control (RBAC) mechanism for creating user, group, and role objects. This makes it easy for you to assign access to applications and data within your instances. Access Control Rules and Lists (ACLs) in conjunction with RBAC let you control access to

entire tables, records, or fields. Several out-of-the box ACLs are included with your ServiceNow instance. You also have the ability to define your own ACLs to suit your needs. The ACLs control individual entitlements around creating, reading, writing, and deleting tables, records, and fields.

Access Control

Administrators of ServiceNow can manage the individuals who can access ServiceNow by defining them as users in the system and assigning them to groups and controlling access to information and functionality. Applications running on the ServiceNow platform can be configured to restrict access to and within applications through role-based access controls at the level of any data object – application, module, table, row, column or field. Multiple identity management interfaces, including SSO, Active Directory, LDAP and SAML, allow IT to control user and role access by leveraging systems already in place. Once users have roles authorizing them access, they can manage information like course catalogs, curriculum, transcripts, and progress reports. Users also have profiles which identify departments/organizational units, skills, and any other custom attributes.

Form security can easily be managed by simple group and role assignments. Administrators can create roles that permit or deny access to users at the field, row or even table level, and then assign these roles to individual users. In addition, security is built into all levels of the system. You can implement the security features that are appropriate for your organization, from managing failed logins and encrypted password protection, to access control rules and audit logs.

ServiceNow provides several audit mechanisms. Within a record, audit history displays all updates and resolution activities that pertain to the record in activity log or calendar format. Enabling auditing tracks the creation, update, and deletion of audited records. All tables within ServiceNow are audited using default auditing capabilities. Time stamp and user ID are associated with system file audits. Code and other script changes can be versioned and compared/reverted if needed.

In addition, Application Logs collect information from the application and are unique to an individual instance. Customers have full access to application log files and are able to download these log files from the application. Events such as user login, failed user logins and privilege escalation are tracked in the log files. The most fine-grained logs are the transaction logs that capture every click, view and action within the system.

Tier 1 Support

ServiceNow offers the same world-class Tier 1 support to every customer. Requests are categorized by priority, with Priority 1 requests receiving fastest response time and highest level of effort. The

Customer Support team is available 24 hours a day, 7 days a week, including all holidays. Customers can submit support requests by phone or through ServiceNow's Customer Support website. Customers can also track the status of requests through the Customer Support website. In addition, quick solution paths can be found using technical support tools such as user forums, blogs, product documentation, and useful solutions. All support tools and materials are available on our websites 24 hours a day.

ServiceNow has a robust monitoring and diagnostics framework based on delivering cloud service to the end user. This framework helps detect, respond, predict, and prevent issues at each layer of the service dependency. When ServiceNow detects an issue that requires Support, it will log a customer-facing Incident via the Customer Service Portal. It will select the Incident priority based on its knowledge. After the accessing the impact, the customer can request that the priority be changed if needed.

Maintenance and Support

Maintenance and support of the PlatCore Learning Management System is provided at no additional cost for installation, configuration and core functionality support. PlatCore releases new versions at no additional cost. When released, new versions are available for download from the ServiceNow Store and our support is available to assist with installations at no additional cost. ServiceNow provides all Tier 1 support for the platform instance environment. PlatCore provides Tier 2 and Tier 3 support for issues related directly to the LMS. Our support team can be reached via email (support@platcore.com) or phone (844-205-7789).

- Low – Monday – Friday, Business hour coverage with response within 1 day and complete issue resolution in 5 days.
- Medium – Monday – Friday, Business hour coverage with response within 1 day and complete issue resolution within 3 days.
- Critical (production environment down) – This is covered under the above ServiceNow Support SLA – they provide 24x7 response in 1 hour with issue resolution in 6 hours.

How to contact us:

Phone support: 844-205-7789
e-Mail support: support@platcore.com
Portal: platcore.service-now.com/csm