Introduction

ServiceNow's security team has compiled a list of frequently asked questions about our cloud security processes and the physical, administrative, and logical controls we have in place.

Please see Securing the Now Platform for more information on ServiceNow’s security program.

Please note, all information in this document is related to the standard Now Platform commercial environment. For information related to ServiceNow’s in-country cloud offerings around the globe and how they may differ, please contact your ServiceNow account representative.
Table of Contents

Data access ............................................................................................................ 5
Who has access to customer data? ................................................................. 5
Which authentication methods are available to customers? ....................... 5
What password policies can customers use? .................................................... 5
How do ServiceNow employees access the cloud infrastructure? .......... 5

Data residency ....................................................................................................... 6
Where is customer data hosted? ................................................................. 6
Where are the data centers located? ............................................................... 6
Can customers have their data stored in a single data center? ................. 6
Can customers use one of ServiceNow's data centers and pair it with
one of their own? ............................................................................................... 6
Is customer data transferred around the world? ............................................ 6

Data backups ......................................................................................................... 6
How is data backed up, and how often? ............................................................ 6
How long is backed up data kept? ................................................................. 6
Are backups encrypted? ....................................................................................... 6
Does ServiceNow take tape backups offsite? ................................................. 6
Can customers restore data if they need to? ................................................... 6

Encryption .............................................................................................................. 7
What options are available for customers to encrypt their data? ................. 7
How is data encrypted in transit? ................................................................. 7

Logging ............................................................................................................... 7
Can customers see ServiceNow's firewall and infrastructure logs? ............. 7
How long are the logs available? ................................................................. 7

Testing .................................................................................................................. 7
Can customers perform load testing? ............................................................... 7
Can customers perform a penetration test on their ServiceNow instance? ... 7
What should customers do if they discover a vulnerability? ....................... 7
Can customers audit ServiceNow? ................................................................. 8

Software updates ................................................................................................. 8
Do software updates and patches happen automatically? ....................... 8
Why do instances need to be patched? ............................................................ 8
When do customers need to upgrade their instances? ............................... 8
Can customers roll back an update? ............................................................... 8

Customer support ............................................................................................... 8
Can customers have in-country only support? ............................................. 8
Can customers have dedicated or named support people only? ............... 8
Mobile applications
What do customers need to know about mobile app security? 9
How can customers control what mobile users can access? 9
How is mobile app data secured? 9

Administrative procedures
How does ServiceNow onboard/offboard its personnel? 9
Can customers perform background checks on ServiceNow personnel? 9
Does ServiceNow use subcontractors? 10
Does ServiceNow perform vendor risk assessments (VRAs)? 10

Compliance and auditing
How can customers find out more about compliance/standards? 10
Is ServiceNow’s information security policy documentation available? 10
Does ServiceNow maintain an ISO/IEC 27001 certification? 10

Miscellaneous questions
How do Customers find their instance IP address? 10
Can ServiceNow help me understand what types of data I have, and whether it falls under privacy laws, e.g. GDPR, PCI-DSS, HIPAA? 10
Can customers install their own hardware/software in ServiceNow’s cloud? 10
Does ServiceNow have a disaster recovery plan? 11
What happens to a customer’s data if they stop being a Customer? 11
How do customers access their database dump? 11
What is ServiceNow’s data destruction process? 11
How can customers communicate with ServiceNow? 11

Resources
Data access

Who has access to customer data?

Customer data can be accessed via both the application and the infrastructure. Customers can control access to their data at the application layer via Access Control Lists (ACLs). Default ACLs are available out-of-the-box and can be customized to suit.

ServiceNow does not require access to customer data via the infrastructure layer during normal service provision. However, if issues arise which cannot be resolved by the platform’s automation capabilities, a ServiceNow cloud administrator may need to access servers or database systems for investigation and resolution. All activity of this type is logged.

ServiceNow support representatives may need access to a customer’s instance to resolve customer-raised issues. Any such application layer access is recorded in the system logs and identified with a username ending in `@snc`.

Customers may prevent application layer access by ServiceNow by enabling the ServiceNow Access Control (SNAC) plugin. SNAC requires explicit approval to be given by the customer before instance access is allowed. Enabling SNAC will delay progress on support activities requiring instance access until the customer grants access.

Multiple preventative and detective controls have been implemented to prevent unauthorized access to infrastructure. These are documented in the SOC 2 Type 2 report which is available to customers in the CORE compliance portal. Find out how to access the CORE Compliance Portal here.

Which authentication methods are available?

Built-in, multi-provider SSO, SAML 2.0, LDAP, OAuth 2.0, Adaptive, and others. More details are available in our product documentation.

What password policies can I use?

Customers can set their own password policies, either in their instance or in the external directory service used for SAML or LDAP.

How do ServiceNow employees access the cloud infrastructure?

Only ServiceNow personnel with a defined and approved support role may access the cloud infrastructure. Access is via regionally-deployed, secure virtual desktop environments. These require two-factor authentication from clients within ServiceNow address space, identified by ServiceNow-issued digital certificates.

All access, authorization, SSH access, and any commands requiring elevated privileges are logged, monitored, and controlled by our centralized Privileged Access Management (PAM) system. Quarterly privilege reviews are undertaken for all relevant personnel.

Host-based Data Leak Prevention (DLP) is enabled, and no internet access, email, messaging, or device and clipboard redirection is possible.

View the ServiceNow Controlled Access (SNCA) Policy in CORE for more information. Find out how to access the ServiceNow CORE Compliance Portal here.

ServiceNow operates data centers in North and South America, Europe, United Kingdom, South East Asia, Japan, and Australia.
Data residency

Where is customer data hosted?
Customer data is hosted in data center (DC) pairs within the region selected by the customer. Regional DC pairs are pre-defined by ServiceNow. There is no defined primary and secondary site within a DC pair, but an individual instance will be served from one of the DCs at any given time until transferred to the other. Data center transfers are transparent to the end-user.

Where are the data centers located?
ServiceNow operates data centers in North America (Canada is the default location, with additional centers in the United States), Asia (South Korea and Singapore), Europe (Germany, Switzerland, The Netherlands, Ireland), U.K. (England and Wales), Japan, Australia, Brazil, and India.

Can customers have their data hosted in a single data center?
By design, customer data is held within pairs of data centers to provide resilience and be highly available. See the Advanced High Availability eBook for a detailed description.

Can customers use one of ServiceNow’s data centers and pair it with one of their own?
ServiceNow provides leading compliance, security, and availability built on a highly standardized platform. Achieving industry-leading availability and security would not be feasible, nor technically achievable, using resources outside of ServiceNow’s own environment.

As such, we do not allow customers to use their own data centers, but customers may choose to export their data into their own environment on a regular schedule.

Is customer data transferred around the world?
No, data always remains in the customer’s designated data center pair. Incidental transfers may take place during support or other relevant interactions with ServiceNow. Transfers are made in accordance with customer contractual and relevant legal obligations.

Data backups

How is data backed up, and how often?
For production instances, data is backed up to disk within that instance's data center pair. Sub-production instances exist in and are backed up to a single data center only. Full backups are taken weekly, with differential backups made daily in between.

See the Backup and Restoration SOP in CORE for more information. Find out how to access the CORE Compliance Portal here.

How long is backed up data kept?
Backups are retained in accordance with our operating procedures, after which no record of deleted data will remain in ServiceNow infrastructure. At the end of their working life, disks are securely wiped or destroyed such that no data remains.

See the Backup and Restoration SOP in CORE for more information. Find out how to access the CORE Compliance Portal here.

Are backups encrypted?
All instance backups are encrypted with AES-256. Unique encryption keys are generated for every backup and are kept in a secure keystore. They are retrieved by an automated process if a data restore is initiated.

Does ServiceNow take tape backups offsite?
Data is backed up to disk, not tape, and remains within the data centers. Production ServiceNow instances are backed up in each data center in a regional pair, each location providing offsite backup storage for the other.

Can Customers restore data if they need to?
Customers can restore data if they need to. However, the Advanced High Availability (AHA) Architecture means that restores are only relevant in specific situations, e.g. if a Customer accidentally deletes data from an instance. Individual items such as tables or fields can be restored from within the platform. Customer Support can assist in the very rare situation where an entire instance needs to be restored as a last resort.
Encryption

What options are available for customers to encrypt their data at rest?

The Now Platform allows several options for encrypting data at rest. Customers may choose a combination of:

• Column Level Encryption (CLE) and CLE Enterprise (CLEE) provides role-based symmetric data encryption for supported data fields.

• Database Encryption protects data in ServiceNow storage in case of physical disk/server loss or theft. Database Encryption encrypts data within the database table; data is only decrypted while it’s being accessed.

• Cloud Encryption protects data in ServiceNow storage in case of physical disk/server loss or theft, Cloud Encryption encrypts the database's storage volume at rest, and ensures compatibility with future database technology enhancements.

• Edge Encryption encrypts or tokenizes data onsite before it is sent to a ServiceNow instance.

• Full Disk Encryption protects data in ServiceNow storage in case of physical disk/server loss or theft, it also uniquely requires customers to also purchase a dedicated environment for hardware encryption.

CLE, CLEE, and Cloud Encryption all use the NIST 800-57 compliant Key Management Framework (KMF), which provides comprehensive key lifecycle management.

More information is available in the ServiceNow Data Encryption eBook.

How is data encrypted in transit?

Data in transit between the customer and ServiceNow is protected with TLS 1.2. We do not support SSL.

Logging

Can Customers see ServiceNow’s firewall and infrastructure logs?

Customers are free to access their own instance’s audit and monitoring logs, but not those of the wider ServiceNow infrastructure, because this could include other customers’ activity. ServiceNow can however, share redacted logs in the case of a security incident.

How long are logs available?

ServiceNow cloud infrastructure logs are retained for a minimum of 90 days, and OS and security logs are maintained for one year.

Testing

Can customers perform load testing?

Customers may perform load testing only by pre-arrangement, and on an isolated environment provisioned specifically for this purpose. This ensures testing can be carried out correctly and without impacting other customers. Please contact your ServiceNow account representative if you would like to request a load test.

Can customers perform a penetration test on their ServiceNow instance?

ServiceNow allows customers to penetration test their instances once per calendar year at no cost provided pre-requisites are met and the test is specifically scheduled and authorized via the Now Support service catalog.

Customers must schedule penetration test in accordance with the Customer Penetration Testing Policy. All security testing outside of this process is expressly forbidden.

What should customers do if they discover a vulnerability?

ServiceNow does not condone any attempts to actively audit our infrastructure. However, we recognize that vulnerabilities in our systems, products, or network infrastructure are occasionally discovered incidentally. If you discover a vulnerability, please report it to us by submitting a Security Finding.
Can customers audit ServiceNow?

As a SaaS vendor, and in keeping with common industry practice, ServiceNow invites its own external auditors to undertake regular, comprehensive audits. The results of these audits can be shared with customers, who may self-serve the relevant documents via the ServiceNow CORE Compliance portal.

Find out how to access the CORE Compliance Portal here.

Software updates

Do software updates and patches happen automatically?

The ServiceNow Patching Program updates customer instances to required patch versions throughout the year. With this program, instances get the latest security, performance, and functional fixes. Most importantly, patching remediates known security vulnerabilities and is an essential component of any patch management process.

Why do instances need to be patched?

Patches improve reliability, availability, performance, and most importantly, security. Version upgrades bring enhanced functionality, improved appearance and usability, as well as other benefits. Security patches help protect all customers collectively, as well as individually.

When do customers need to upgrade their instances to the latest version?

Major platform version updates are typically released twice per year, with one full patch version each quarter and two incremental security patches each quarter. ServiceNow will notify customers in advance when they should update. Customers must comply with the ServiceNow Patching Program to ensure continuous support. ServiceNow provides support for the current release version and one release prior (N-1).

Can customers roll back an update?

All updates, patches and hotfixes undergo extensive and rigorous testing before release to ensure compatibility and reliability. However, should you need to roll back an update for any reason, you can do so by contacting Customer Support within a configurable window (10 days by default).

Customer support

Can standard commercial customers have in-country only support?

For information about a specific ServiceNow in-country cloud offering, please discuss specific support options with your account representative.

US-only support is available for a fee for any entity that requires their support to be exclusively provided by ServiceNow US Person/US Soil personnel. In all other regions, ServiceNow provides the option of 24/7 Customer support - with 12/5 as the standard offering - using a ‘follow-the-sun’ model. This entails provision from different global locations throughout the day. These locations are: San Diego, Kirkland, London, Amsterdam, Orlando, Sydney, Hyderabad, Dublin, and Tokyo.

Can customers have dedicated or named support people only?

Qualified personnel are assigned to incidents, rather than individual customers, based on demand and availability. Customers can use the ServiceNow Access Control plugin to control who may access their instance during a specific incident.
A customer may also optionally subscribe to the Support Account Manager service for a dedicated point of contact for support and other relevant matters. Contact your ServiceNow account representative for further information.

Mobile applications

What do customers need to know about mobile app security?
ServiceNow has developed new native mobile apps for iOS and Android. These apps use OAuth 2.0 and benefit from the robust authentication mechanisms (optionally augmented with multi-factor authentication) that customers already use with ServiceNow, including SAML, LDAP, Adaptive authentication, and local authentication, along with AppAuth.

Security information on these new mobile applications along with configuration best practices can be found in our Mobile security overview.

How can customers control what mobile users can access?
Once authenticated, user sessions are managed with access tokens and mobile users are subject to the same access controls as any other users.

How is mobile app data secured?
All data in transit is protected with TLS 1.2 and app preference information is encrypted with AES-128. By default, no customer record data is stored on the mobile device, though this is configurable. More information on mobile security can be found in our Mobile security overview.

Administrative procedures

How does ServiceNow onboard/offboard its personnel?
Onboarding: ServiceNow human resources security starts at the very beginning of the employment process with ServiceNow. Mandatory screening includes criminal, employment, financial, citizen checks, and government watch lists, as well as drug tests in applicable jurisdictions. Failure to pass these tests will result in disqualification or a follow-up investigation, depending on the nature of the non-compliance.

Once employed, every new member of staff must sign a non-disclosure agreement, sign the ServiceNow Code of Conduct and Ethics Agreement, read and accept the ServiceNow Acceptable Use Policy, and undergo annual security training and compliance training.

Offboarding: ServiceNow has a standard operating procedure that involves both HR and IT. When an employee is departing, HR informs IT of their last day of service and based on their role, IT removes their access. The stated time to do this is within 24 hours of the employee leaving, however, in practice it generally happens much sooner than this.

Can customers perform background checks or other vetting on ServiceNow personnel?
This is not possible due to legal and other obligations towards ServiceNow employees. However, ServiceNow performs extensive background checks and training for our personnel as part of our ongoing compliance accreditations and certifications. Customers may in some circumstances request proof for individuals, for example in the event of a professional services engagement.
Does ServiceNow use subcontractors?
All equipment is owned and managed by ServiceNow and held within ServiceNow-owned and managed cages or suites. This includes servers, network equipment, storage infrastructure, and security solutions. External network connectivity is direct from the provider to our assigned cage/suite, and network traffic does not traverse the hosting data center’s network equipment. ServiceNow has a very small number of onsite personnel globally with access to manage our data center equipment.

Does ServiceNow perform vendor risk assessments (VRAs)?
ServiceNow performs VRAs and relevant third-party vendors are reviewed for compliance as part of our vendor management program. This process is owned by a dedicated VRA compliance team, who ensure that the appropriate level of assessment is conducted according to the types of services and assets involved. The compliance team works with the vendors and with internal SMEs to perform the assessment. This results in a vendor risk assessment report, which is reviewed and either approved or rejected by the executive management team.

For more information, customers with access to ServiceNow CORE can review the ServiceNow Vendor Risk Assessment SOP. Find out how to access the CORE Compliance Portal here.

Compliance and auditing

How can customers find out more about ServiceNow compliance and standards?
Publicly available information about compliance can be found on the Compliance page of the ServiceNow Trust site.
Customers and partners can be granted access to ServiceNow CORE in Now Support to see evidence of ServiceNow’s certifications, standards, procedures, SOC Reports, pre-filled vendor risk questionnaires etc.
Companies wishing to evaluate ServiceNow as a vendor may also be granted time-limited CORE access.
Find out how to access the CORE Compliance Portal here.

Can I see your information security policy documentation?
ServiceNow has a very detailed set of information security policies and standards that are based on ISO 27001 and assessed as part of this certification. ServiceNow’s information security policy is reviewed and approved by the CISO at least annually and is owned by the director of governance, risk management, and compliance at ServiceNow.
ServiceNow’s information security policy can be found in CORE. Find out how to access the CORE Compliance Portal here.

Does ServiceNow maintain an ISO/IEC 27001 certification?
Find out more about ServiceNow certifications on the Compliance page of the ServiceNow Trust site.

Miscellaneous questions

How do customers find their instance IP address?
Customer instances use IP addresses from an 8-address (/29) subnet. Find out more about identifying the IP of your instance here.

Can ServiceNow help me understand what types of data I have, and whether it falls under privacy laws, e.g. GDPR, PCI-DSS, HIPAA?
The Data Classification feature allows customers to understand where specific data is present within their Now Platform instances, and to report on or create dashboards to better understand data categories in use. This assists in meeting statutory or regulatory requirements such as GDPR, PCI-DSS or HIPAA.

Can customers install their own hardware or software in the ServiceNow cloud?
As is the case with most cloud providers, it is not possible for customers to install their own hardware or software in the ServiceNow cloud. Instances of the Now Platform are delivered using a completely standardized cloud infrastructure. The entire environment is under the complete control and management of ServiceNow on behalf of its customers. Now Platform instances are very flexible.
and can be configured and customized as required, including the use of customer-generated code.

**Does ServiceNow have a disaster recovery plan?**

ServiceNow operates a disaster recovery (DR) program for customer environments called the information system contingency plan (ISCP). In the event of a disaster, ServiceNow activates a failover process that transfers customer operations to the unaffected data center. In this model, the targeted recovery point objective (RPO) and recovery time objective (RTO) durations are one and two hours, respectively.

The ISCP is tested annually and the results are documented in the ISCP test report. The exercise scenarios are designed to test Advanced High Availability (AHA) failover to a secondary data center as well as recovery from backup. These procedures are often completed well within expected RPO and RTO windows as transfers between data centers are also performed for maintenance purposes, making this a highly practiced process for ServiceNow.

The latest ServiceNow Information System Contingency Plan Test Report can be found in the ServiceNow CORE Compliance Portal.

Find out how to access the ServiceNow CORE Compliance Portal [here](#).

**What happens to a customer’s data if they stop being a customer?**

Upon termination or expiration of the agreement with ServiceNow, customers may request the return of all Customer data within 45 days. Data is returned using an industry standard format by means of a database dump. After that time, the data is logically wiped from the system following the NIST 800–88 guidelines.

**How do customers access their database dump?**

Customers can only obtain your data by downloading it from our secure file transfer service, which uses FTPS to keep the transmission secure. No other method is available.

**What is ServiceNow’s data destruction process?**

ServiceNow logically sanitizes mechanical and solid-state drives (SSD). We follow a data sanitization standard operating procedure (SOP) to destroy data on mechanical disks. This process is consistent with NIST 800–88, Guidelines for Media Sanitization, and NISP Operating Manual (NISPOM) DOD 5220.22–M.

The Media Sanitization & Hardware Destruction SOP can be found on the ServiceNow CORE Compliance portal.

Find out how to access the ServiceNow CORE Compliance Portal [here](#).

**How can customers communicate with ServiceNow?**

All communication between ServiceNow and its customers is conducted via the Now Support service portal or your support account manager (SAM) if you have one. This ensures that your queries are captured, prioritized, and routed efficiently without reliance on individual availability.

ServiceNow is committed to GDPR compliance across our enterprise cloud services. We believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights.
Resources

There is a wealth of information available online in the following publicly accessible locations:

- Product Documentation
- Community Support
- ServiceNow Trust Site

Existing Customers can also access the following resources:

- CORE
- Trust and Compliance Center
- General Technical Support
- ServiceNow Security Best Practice Guide