Safeguarding Your Data
An overview of data security at ServiceNow
Release: Washington, DC
Introduction

The Now Platform® features security by design, giving customers the tools and procedures necessary to protect their data from unauthorized access or change. All of this is accomplished while retaining the class-leading, high availability of the Now Platform cloud environment.

For an overview of the ServiceNow® security program, please refer to the Securing the Now Platform white paper.

This document discusses how different data types are handled, and the responsibilities of the data controller (ServiceNow customers) and the data processor (ServiceNow). It also gives an overview of what controls ServiceNow provides to assist customers in keeping their data safe.

Please note: all information in this white paper is related to the standard Now Platform commercial environment.

For information related to other globally located ServiceNow in-country cloud offerings and how these offerings may differ, please contact your ServiceNow account representative.
# Table of contents

## Introduction ......................................................... 2

## Security and privacy considerations
  by use case ....................................................... 5
  - IT Service Management (ITSM) security considerations .... 5
  - IT Operations Management (ITOM) security considerations .... 5
  - IT Business Management (ITBM) security considerations .... 5
  - Human Resources (HR) security considerations .......... 6
  - Customer Service Management (CSM) security considerations .... 6
  - Security Operations product security considerations .... 6

## Data considerations ............................................... 7
  - Data roles and responsibilities .................................... 7
  - Data controller *(the customer)* ...................................... 7
  - Data processor *(ServiceNow)* ....................................... 7
  - ServiceNow Shared Responsibility Model ...................... 7
  - Data sovereignty ..................................................... 8

## Data privacy ....................................................... 8
  - What is data privacy? .................................................. 8
  - Protecting personal data ............................................... 8
  - Data privacy operations .............................................. 9
  - Data return and destruction ......................................... 10

## Asset data .......................................................... 11
  - Managing asset data .................................................. 11
  - Storing CMDB data and related information in the cloud .... 11
  - Now Platform MID Server ............................................ 11
## Accessing Data

- Customer access to data. ........................................... 12
- ServiceNow access to customer data .......................... 12

## Technical controls

- Overview of authentication and authorization ............. 12
- Overview of logging and monitoring .......................... 13
- Secure communication with the instance ................. 13

## Conclusion

................................................................. 14

## Additional resources

................................................................. 14
Security and privacy considerations by use case

At ServiceNow, we take great pride in providing a market-leading platform that enables businesses to work more efficiently and effectively.

ServiceNow believes it is essential to understand the data security needs, and concerns, associated with relevant use cases to provide industry-leading security for the Now Platform. The key considerations are outlined below. Many of them are common across multiple scenarios.

**IT Service Management (ITSM) security considerations**

IT departments handle large quantities of data daily, including requests related to incidents, problems, and changes, such as password resets, computer hardware issues, patch management, and maintenance. As well as information pertaining to applications, systems, services, information assets, and infrastructure managed within ITSM is stored in the Configuration Management Database (CMDB).

Effective ITSM relies on maintaining accurate data and connecting business users, assets, processes, and more. Securing all aspects of that integration is essential. ServiceNow understands that processes involving user-generated data can sometimes cause additional unnecessary (but sensitive) information to be collected. When this occurs, that additional information also requires identification and protection.

The data assets stored in the CMDB include information about the organization’s internal infrastructure and IT-related assets, such as server models, OS versions, patch levels, dependencies, and IP addresses. Attackers could potentially use this key configuration data to identify vulnerabilities in a system.

While not directly enabling attacks, detailed maps of corporate infrastructure should be considered sensitive information. For this reason, it is vital that all data stored in the CMDB is properly protected at all times.

**IT Operations Management (ITOM) security considerations**

Like ITSM, ITOM activities also handle large quantities of critical data, which may include user credentials. Protecting these assets is fundamental to the security of an organization.

It is also important that communication with Now Platform instances is secure, that role-based access controls are correctly implemented, that access to the instance is appropriately secured, and that special consideration is given to the storage and management of credentials used to support ITOM.

Integration of customer systems and services with Now Platform instances is enabled through secure integrations and deployment of components such as the ServiceNow MID Server and Secrets Management.

**IT Business Management (ITBM) security considerations**

ITBM involves financial, strategic, and resourcing information. Maintaining and securing accurate information about links between business users, assets, and processes is essential. Collecting user-generated freeform information can sometimes result in the capture of unnecessary and sensitive data — the associated risk must also be identified, and mitigated, where possible.

ITBM data is considered sensitive, as it encompasses budgets, costs, and other financial information. It may also include data related to personnel, business strategy or intellectual property, and could include asset data. This information must be secured and accessible only to authorized personnel and systems.

“ServiceNow believes it is essential to understand the data security needs and concerns associated with relevant use cases to provide industry-leading security for the Now Platform.”
Human Resources (HR) security considerations

HR organizations store and process a wide variety of highly sensitive personal data, such as ID numbers, copies of passports, disciplinary data, or medical history. HR teams have a unique and important function within any organization.

Due to the sensitive nature of the data connected to HR requests, ServiceNow ensures that only authorized HR personnel can access such sensitive, personal information. Even the IT system administrators must be authorized to access the HR application’s data.

HR departments typically use multiple systems and applications to manage core HR, benefits, payroll, recruiting, talent management, employee documents, and communications — sometimes all separately.

Secure integrations into these existing systems are vital. The Now Platform currently supports a wide range of integration methods with third-party HR applications.

Customer Service Management (CSM) security considerations

ServiceNow offers a powerful CSM application on the Now Platform, which can unlock almost limitless possibilities for a company wanting to interact with its customers directly. Common requests, such as changes to personal details, password resets, and warranty registrations, can all be automated.

The CSM application is likely to handle large amounts of personal information. Any compromise of this data’s confidentiality, integrity, and availability could have severe consequences, especially in the case of highly sensitive information. ServiceNow adheres to information security best practices in protecting this data.

Customers can browse service catalog items, request assistance, and participate in community groups to share experiences and solve problems. This functionality raises additional considerations for securing customer data. In particular, controls must be in place to manage users’ identification, authentication, and authorization while keeping public and private access separate at all times.

Security Operations product security considerations

ServiceNow fully understands the security-based activities that protect customers’ environments and data because it uses the same practices to secure its private cloud and internal corporate environments.

Protecting the environment and data during these activities is an essential component of a comprehensive approach to security. By their nature, the activities produce sensitive information about the organization.

Information collected about vulnerabilities, threat vectors, security incidents, patches, remediation, and the assets involved is highly sensitive and must be protected to reduce risk and exposure.

The Now Platform Security Operations application integrates with many commercially available security tools customers already use. The Now Platform augments these tools to apply business service mapping and workflow automation. Mature organizations undertake security incident response, vulnerability management, threat intelligence, or Governance Risk and Compliance (GRC) programs.
Data considerations

Data roles and responsibilities

In data privacy terms, there are two defined roles, each with its own associated responsibilities. In the case of a customer using the Now Platform, the customer is the data controller, and ServiceNow is the data processor.

• The **data controller** is a person or legal entity who determines why and how the data is used.

• The **data processor** is a person or legal entity that carries out the processing of that data on behalf of the data controller.

The following are additional terms applicable to data privacy:

• A **natural person** is a living individual, as opposed to a legal entity, such as a business.

• A **data subject** is a natural person about which information is being processed.

**Data controller (the customer)**

As the **data controller**, the customer is responsible for determining how data is collected, stored, used, shared, and for maintaining the accuracy and confidentiality of that data. The customer is also responsible for meeting the requirements of the legislation in the jurisdictions in which they operate for collecting data and for demonstrating compliance with applicable local and international laws.

The **data controller** has wider legal obligations and determines the following:

• The purpose of collecting the data

• What data is collected

• How the data is used

• How long the data is retained

• Where the data is stored

• Who the data processor is

**ServiceNow Shared Responsibility Model**

<table>
<thead>
<tr>
<th>Area of Responsibility</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure configuration of instance</td>
<td>Customer: ●</td>
</tr>
<tr>
<td>Authentication and authorization</td>
<td>ServiceNow: ●</td>
</tr>
<tr>
<td>Data management (classification and retention)</td>
<td>Colocation: ●</td>
</tr>
<tr>
<td>Data encryption at rest</td>
<td>●</td>
</tr>
<tr>
<td>Data encryption in transit</td>
<td>●</td>
</tr>
<tr>
<td>Encryption key management</td>
<td>●</td>
</tr>
<tr>
<td>Security logging and monitoring</td>
<td>●</td>
</tr>
<tr>
<td>Secure SDLC processes</td>
<td>●</td>
</tr>
<tr>
<td>Penetration testing</td>
<td>●</td>
</tr>
<tr>
<td>Vulnerability management</td>
<td>●</td>
</tr>
<tr>
<td>Privacy</td>
<td>●</td>
</tr>
<tr>
<td>Compliance: regulatory and legal</td>
<td>●</td>
</tr>
<tr>
<td>Employee vetting or screening</td>
<td>●</td>
</tr>
<tr>
<td>Physical security/environment controls</td>
<td>●</td>
</tr>
<tr>
<td>Cloud infrastructure security management</td>
<td>●</td>
</tr>
<tr>
<td>Infrastructure management</td>
<td>●</td>
</tr>
<tr>
<td>Media disposal and destruction</td>
<td>●</td>
</tr>
<tr>
<td>Backup and restore</td>
<td>●</td>
</tr>
<tr>
<td>Business continuity and disaster recovery</td>
<td>●</td>
</tr>
</tbody>
</table>

**Data processor (ServiceNow)**

The **data processor** (ServiceNow) supports the data controller by providing features to enable access and control of data processing activities and obligations, which includes maintaining and searching data processing records, implementing necessary security measures, notifying the controller in the case of a data breach, and directing any lawful requests made by authorized parties to the controller.

The **data processor** has the following accountability obligations:

• Supports the controller

• Processes data on behalf of the controller

• Ensures confidentiality

• Ensures technical and administrative measures are in place to protect the data

• Enables the keeping of data processing records

• Informs the controller of any data breaches

Security is a shared responsibility between the provider and customer. Please see the [Shared Responsibility Model Overview](#) for more information. ServiceNow offers cooperation and assistance to data controllers (the customer) to ensure compliance with the data controllers’ obligations pursuant to applicable data protection laws. For more details, see the ServiceNow [Data Processing Addendum](#).
Data sovereignty

Data is subject to the laws of the country in which the data is physically stored and to the jurisdiction to which the data subject belongs (e.g. in the case of GDPR).

ServiceNow ensures that data is hosted in regional pairs, where both members are either within the same jurisdiction or within mutually compatible jurisdictions so that even when data is transferred from one data center to another, the sovereignty of the data is preserved.

Data privacy

What is data privacy?

Data privacy addresses the rights of an individual over personally identifiable information (PII) held about them. This type of information is often subject to strict regulation.

PII refers to any information that relates to a living person, such as a person’s name, date/place of birth, social security number, and biometric data. Sensitive personal information (SPI) is an extension of PII which includes sensitive data such as ethnic origin, political opinions, health information, and criminal record. In some jurisdictions, there are additional classifications of SPI, such as protected health information (PHI) in the U.S., which relates to an individual’s health status or healthcare.

Some data items that cannot be used individually to identify a person could still be classified as personal information when used in combination with other information (e.g. age, gender, and address).

Protecting personal data

Personal data must be protected from unauthorized access or data loss. Here are some examples of data protection capabilities of the Now Platform:

- Proper user authentication and authorization
- Anonymize specific data
- Encrypt specific fields categorized as PII, etc.
- Allow users to manage passwords
- Prevent access by users with an inactive account

ServiceNow maintains controls that meet the objectives stated in ISO 27001, 27017, 27018, 27701, SSAE18/SOC 1, SOC 2 Type 2, and APEC PRP for the information security management system supporting the subscription service. At least once per calendar year, ServiceNow obtains an assessment against the standards by an independent third-party auditor.

Additionally, ServiceNow provides the self-serve ServiceNow CORE Compliance Portal to help customers conduct Data Protection Impact Analyses (DPIA), if required.
Data privacy operations

Data subjects have basic rights to privacy. The responsibility for upholding and supporting these rights is shared between the data controller (the customer) and the data processor (ServiceNow).

The EU GDPR (European Union General Data Protection Regulation) is currently the highest standard of data privacy regulation globally, and serves as a useful benchmark for operations related to data privacy.

ServiceNow provides data controllers (customers) with the ability to access, correct, rectify, erase or anonymize personal data – or the ability to transfer (or port) such personal data within the subscription service, as may be required under data protection laws (collectively called data subject requests). However, it is the responsibility of the data controller (the customer) to respond to data subject requests.

The following table outlines the legal rights of an individual and how ServiceNow can be used to support these rights:

<table>
<thead>
<tr>
<th>Individual’s rights</th>
<th>Description and how ServiceNow supports these rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to be informed</td>
<td>Data subjects must be informed that their data is being collected and how it will be used. The Now Platform can be used to automate and record the delivery and acceptance of privacy notices. Basic platform features allow recording and reporting on processing activities. These activities are entirely the responsibility of the data controller (customer).</td>
</tr>
<tr>
<td>Right of access</td>
<td>Data subjects may request information regarding their personal data from the data controller (customer) free of charge, and this should normally be supplied within one month of receipt. If Subject Access Requests (SARs) are made to ServiceNow, they will be redirected to the data controller (customer) without undue delay. Comprehensive search and reporting features allow immediate identification and presentation of data relating to individual subjects, and ServiceNow supports a large variety of output formats and integrations in order to meet this obligation. These activities are entirely the responsibility of the data controller.</td>
</tr>
<tr>
<td>Right to rectification</td>
<td>Data subjects may request that inaccurate personal data is rectified. They must be informed where this inaccurate data has been disclosed to third parties and these third parties must be informed of the rectification where possible. ServiceNow has comprehensive logging features which allow the data controller (customer) to determine when data has been changed, and by whom, and produce complete audit trails where enabled. Web services integrations allow real-time integrations with third parties where necessary. These activities are entirely the responsibility of the data controller.</td>
</tr>
<tr>
<td>Right to erasure</td>
<td>Data subjects may request the deletion or removal of personal data where there is no compelling reason for its continued processing, e.g., the individual withdrawing consent. The data controller (customer) is fully responsible for the erasure of data. ServiceNow has comprehensive auditing and reporting features that can provide visibility into such data and evidence of erasure. ServiceNow is responsible for ensuring that data deleted from customer instances is reflected in all locations where this data is stored. Once data is deleted from the active instance, it is very quickly reflected in the corresponding passive Data Center (DC), and that data will no longer be backed up. Backups are retained in accordance with our operating procedures, after which no record of deleted data will remain in ServiceNow infrastructure. (To view the operating procedures find out how to access the ServiceNow CORE Compliance Portal here.) At the end of their working life, disks are securely wiped or destroyed such that no data remains. With the ServiceNow Data Anonymization feature, customers can anonymize data of data subjects who assert their right to erasure. This feature allows customers to replace the confidential or personally identifiable information (PII) of selected user records with random values, or values defined by the administrator. Customers can also de-identify users when cloning a production instance to a non-production instance. This allows customers to use data for such tasks as application development and testing, while ensuring personal and confidential information privacy.</td>
</tr>
<tr>
<td>Individual's rights</td>
<td>Description and how ServiceNow supports these rights</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Right to restrict processing</td>
<td>Data subjects may request that specific processing be blocked. Restricting processing is a wide-reaching topic that may involve many variables. ServiceNow has a flexible database and data classification system that allows easy tagging of individual records and conditional processing (i.e., respecting a “do not share” restriction and reporting on such activities or restrictions). These activities are entirely the responsibility of the data controller (customer).</td>
</tr>
<tr>
<td>Right to data portability</td>
<td>Data subjects may request to obtain and reuse their personal data for their own purposes, and must be able to transfer the data easily and securely. ServiceNow supports a wide variety of structured data formats, including common open formats such as CSV, XML, JSON, etc. The ability to extract data in different forms is a built-in feature supported universally throughout the Now Platform, allowing data controllers to comply with this requirement easily. These activities are entirely the responsibility of the data controller (customer).</td>
</tr>
<tr>
<td>Right to object</td>
<td>Data subjects have the right to object to processing, and individuals must be clearly informed of this right at the first point of communication. Informing data subjects of this right, at the first point of communication, can be automated and recorded using the Now Platform. These activities are entirely the responsibility of the data controller (customer).</td>
</tr>
<tr>
<td>Rights related to automated decision-making and profiling</td>
<td>Automated decision-making and profiling rights introduce safeguards against the risk of a potentially damaging decision being taken without human intervention. The comprehensive workflow engine of the Now Platform allows for comments, approvals, conditional processing, and multi-channel integration with human decision-makers, allowing data controllers (customers) to build processes that comply with this right. Existing platform auditing and reporting features allow the easy identification of events and individuals subject to specific processes covered by this right. These activities are entirely the responsibility of the data controller.</td>
</tr>
</tbody>
</table>

**Data return and destruction**

Throughout the lifetime of the subscription, data can be directly exported using features available in a Now Platform instance.

Exports of data can be via the user interface, through integrations, or by using optional Now Platform components, such as the available ODBC (Open Database Connectivity) connector or MID Server.

At all times during the term of the contract and prior to termination, or expiration of the agreement with ServiceNow, customers can self-export their data from their instance using features in the Now Platform, or they may request that ServiceNow export their data in a standard format. Please see [Exporting Data](#) from the product documentation for more details.
Asset data

Managing asset data

Asset data refers to both direct and related information about an asset, security event data, vulnerability information, stored credentials for discovery and orchestration, and other similar data types.

The IT Infrastructure Library (ITIL) is a globally recognized best practice framework for information technology service management (ITSM). This framework recommends the use of a software-based Configuration Management System (CMS) to manage infrastructure and asset data.

The CMS contains information about configuration items (CI), such as physical or virtual computer systems, network infrastructure devices, printers, mobile devices, and installed software. This, together with related information, forms a configuration management database (CMDB). The accuracy and integrity of CI data is critical for effective ITSM.

Within a customer instance of the Now Platform, the CMDB is a single, authoritative source of customer infrastructure and asset data. It can be integrated with other systems and processes to enable services such as an IT help desk or capacity and performance management. Other uses include the Now Platform service mapping function, and vulnerability response application.

Storing CMDB data and related information in the cloud

A common concern over storing assets and related information in the cloud is that if compromised, internal IP & MAC addresses, host names, software/firmware versions, or locations of systems or services could be used maliciously to identify vulnerabilities and enable attacks against the infrastructure.

These risks are often overstated, since access to the internal network is required before the data can be used. Skilled attackers would be able to easily determine this information for any network they had compromised by themselves, without the need to first attack a secure CMDB.

Nevertheless, ServiceNow understands the sensitivity and importance of CMDB data, and that it should remain available and accurate at all times.

For this reason, ServiceNow employs an array of security features to protect the confidentiality, integrity, and availability of this data.

More information about these controls is available in Securing the Now Platform.

Now Platform MID Server

ServiceNow Management, Instrumentation, and Discovery (MID) servers allow secure, controlled communication between customer instances and their internal network services. MID Servers are installed and configured by customers to operate entirely within their infrastructure.

MID server activities can be limited using network and administrative controls, including credential management systems. MID servers run commands generated on the Now Platform instance by appropriately credentialed customer administrators. Then, those commands are placed in a fully auditible event queue, which can be inspected and monitored in real-time using built-in features. Restrictions can be placed on the commands used and on the rights of individuals to see and modify commands.
Events are retrieved every 15 seconds via a secure Transport Layer Security (TLS) channel between the MID server and its cryptographically paired parent instance. Credentials provided locally, or passed along with the command, are used to issue the command and record any response. Response data is returned to the instance and stored appropriately.

**Accessing Data**

**Customer access to data**

As the data controller, the customer determines who has access rights to their instance and the data stored in it. As the data processor, ServiceNow provides the tools for customers to secure and audit their instance according to their requirements.

In general, ServiceNow does not access customer data, but it is sometimes necessary during the course of resolving a customer support ticket.

**ServiceNow access to customer data**

Occasionally, ServiceNow employees may be required to access a customer’s instance to provide support. Access to a customer’s instance is on an incidental, per-event basis, and not every customer support event will require access to customer data.

Only members of the ServiceNow support organization who have been specifically assigned to an active incident can be granted access — and that access is granted on a just-in-time basis. Additionally, customers may specify that their explicit authorization is also required when that access is requested.

Access can only be obtained via a secure virtual desktop environment accessible only from ServiceNow data centers, requiring a client device authenticated by a digital certificate.

Users are required to pass two-factor authentication before access is granted. Host-based Data Leak Prevention (DLP) is in place, and user activity is monitored and controlled with a Privileged Access Management (PAM) system.

More information regarding access control can be found in [Securing the Now Platform](#).

**Technical controls**

**Overview of authentication and authorization**

Customers can integrate their Now Platform instances with existing authentication services if required, including services that use directory or single sign-on (SSO) technologies, such as LDAP, OAUTH2, and SAML, with or without MFA. Identity management with SCIM is also supported.

The latest releases of the Now Platform have introduced adaptive authentication and zero trust access to further control access based on multiple attributes, user context and limited time authentication. Adaptive authentication and zero trust access enable user accounts to be managed within the customers’ existing processes and standards. Alternatively, customers can define roles and groups within the Now Platform instance.

Once authenticated, the Now Platform’s role-based access control system (RBAC) allows customers to control access to data and functionality within their instance. The ServiceNow RBAC is based on users, groups, and roles.

The permissions granted to users are created from Access Control Lists (ACLs). ACLs can be built from individual permissions that include read, write, create, execute, and delete, as well as a number of other individual attributes. Available attributes vary based on the type of object being secured.

Customers have complete control of the permissions being granted to each of their users, and integration with directory services is possible with users, groups, and group membership.
Overview of logging and monitoring

An audit log records most activities within an instance, and the Now Platform includes comprehensive access, event, and transaction logging.

- The extent of logging is customer-configurable. Customers can use detailed logging to record and report on all activity within an instance.
- Customers can review logs directly in their Now Platform instance, or export them via a MID server to a customer’s security information and event management (SIEM) tool. Workflows or incidents can be automatically created based on detected activity.
- Customers can also enable auditing for database tables to track and view details of any changes made to data at a record or field level.
- Options are available for direct customer SIEM integration, facilitating real-time logging as part of the ServiceNow Vault security bundle.

To detect potentially malicious actions or activities on instances of the Now Platform, ServiceNow collects and retains logs and events relevant to its entire cloud infrastructure, including information regarding requests made to the Now Platform.

ServiceNow uses such log and event management with its ongoing operational security and incident management processes. This information is not available to customers within their ServiceNow instances.

However, events that occur within a specific customer’s instance are accessible to that customer through their instance logs.

These events are also captured in the ServiceNow infrastructure logs.

<table>
<thead>
<tr>
<th>Log type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td>All browser activity for an instance</td>
</tr>
<tr>
<td>Email and push</td>
<td>All email notifications and push messages sent from all instances within the system</td>
</tr>
<tr>
<td>Events</td>
<td>All system events that occur within the system</td>
</tr>
<tr>
<td>Imports</td>
<td>Data import activity within the platform</td>
</tr>
<tr>
<td>Table changes</td>
<td>Changes made to all tables in the system</td>
</tr>
<tr>
<td>Outbound HTTP requests</td>
<td>All outbound web services requests, such as REST and SOAP requests</td>
</tr>
<tr>
<td>Signature images</td>
<td>Electronic signatures for the HR signature pad</td>
</tr>
<tr>
<td>System</td>
<td>Warnings and errors for instance processes, records, and non-critical events, such as memory usage on the server machine</td>
</tr>
</tbody>
</table>

Secure communication with the instance

By their nature, customer instances of the Now Platform are designed to be accessible via the internet, providing maximum flexibility in how, when, and from where they are accessed.

However, the internet is a public network; therefore, attackers could intercept (and read) communications if they are not encrypted or otherwise protected.

ServiceNow provides transport layer encryption as standard within its cloud infrastructure. The Now Platform enables customers to use its encryption in transit capabilities when integrating with their own external systems, data sources, or services.

Customers access their instances via a web browser using Transport Layer Security (TLS) encryption using AES with 128-bit or 256-bit cipher suites. Any data transferred from the on-premises MID server to the Now Platform uses the same TLS encryption.

All end-user access to a ServiceNow instance attempted over HTTP is redirected to HTTPS.

Negotiated ciphers are subject to customer browser versions and may be influenced by customer internet proxy infrastructure. Customers can force specific cipher suites via their own browsers or proxies if desired.

For additional security, customers can also use IP range-based authentication to restrict which public networks are used to access their Now Platform instances.

The standard contractual clauses are applicable as a data transfer mechanism, as per section 9 (international data transfers) of the ServiceNow Data Processing Addendum.
Conclusion

ServiceNow provides customers with a secure environment to store and process their data.

This document has examined the types of data involved, the roles and responsibilities of both the data controller (the customer) and the data processor (ServiceNow), and who can access data in an instance.

Security controls available to customers that can enforce, audit access, and protect Now Platform instances have also been explored.

For more information about how ServiceNow secures the Now Platform, check out the white paper on Securing the Now Platform.

Additional resources

- [ServiceNow Trust Site — Privacy](#)
- [Securing the Now Platform](#) white paper
- [Data Encryption](#) white paper
- [ServiceNow legal schedules](#)
- [Information security policy](#) on the ServiceNow CORE Compliance Portal (requires access)
- [Data protection policy](#) on the ServiceNow CORE Compliance Portal (requires access)

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