Safeguarding Your Data
An overview of data security
Introduction

The cloud represents a leap forward in capability and value. When viewed from a data-centric perspective, it can also represent a leap forward in security. Ensuring confidentiality, integrity, and availability of customer data at all times is of paramount importance.

The Now Platform® features security by design and provides customers with the tools and procedures necessary to protect their data from unauthorized access and change, while retaining the class-leading, high availability of its cloud environment. For an overview of the ServiceNow security program, please refer to the Securing the Now Platform eBook.

This document discusses different types of data, how it is handled, and the responsibilities of the data controller (ServiceNow customers) and 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 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

**Introduction** ..............................................................................................................................2

**Security and privacy considerations by use case** ........................................................................4

IT service management (ITSM) security considerations....................................................................4
IT operations management (ITOM) security considerations............................................................4
IT business management (ITBM) security considerations ............................................................4
Human resources (HR) security considerations ............................................................................5
Customer service management (CSM) security considerations ....................................................5
Security operations product security considerations .......................................................................5

**Data considerations** ....................................................................................................................5
Data roles and responsibilities ...........................................................................................................6
Data sovereignty ...................................................................................................................................6

**Data privacy** ..................................................................................................................................6
What is data privacy? ..........................................................................................................................6
Protecting personal data ....................................................................................................................7
Data privacy operations ....................................................................................................................7
Data return and destruction ..............................................................................................................9

**Asset data** ..................................................................................................................................9
Managing asset data........................................................................................................................9
Storing CMDB data and related information in the cloud .................................................................9
ServiceNow orchestration and discovery .......................................................................................9

Data used for machine learning and artificial intelligence ............................................................10
Data used for machine learning .....................................................................................................10
The DART program (Data Access for Responsible Training) .......................................................10

**Accessing Data** ..........................................................................................................................10
Customer access to data ................................................................................................................10
ServiceNow access to customer data .............................................................................................10

**Technical controls** ....................................................................................................................11
Overview of authentication and authorization ..............................................................................11
Overview of logging and monitoring ............................................................................................11
Secure communication with the instance ......................................................................................12

**Conclusion** ..................................................................................................................................12

**References** ..................................................................................................................................12
Security and privacy considerations by use case

At ServiceNow, we take great pride in providing a market-leading platform that enables business to work more efficiently and effectively. To provide industry-leading security for our platform, we believe it is essential to understand the data security needs and concerns associated with relevant Now Platform® use cases.

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. This data includes requests related to incidents, problems, and changes, such as password resets, computer hardware issues, patch management, and maintenance. Information related to applications, systems, services, information assets, and infrastructure managed within ITSM is stored in the configuration management database (CMDB).

Effective ITSM relies upon maintaining accurate data and connecting business users, assets, processes, and more. Securing all aspects of that integration is essential. We understand 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 internal infrastructure of the organization and IT-related assets, such as server models, OS versions, patch levels, dependencies, and IP addresses. This key configuration data could be easily used 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 essential to the security of the 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.

**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—this 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 may also include asset data. This information must be secured and accessible only to authorized people and systems.

**Human resources (HR) security considerations**

HR organizations store and process a wide variety of personal data that is of a highly sensitive nature, such as ID numbers, copies of passports, disciplinary data, or medical history. Employees may also confide in HR representatives about personal matters, including mental health and work/life balance. HR teams have a unique and important function within any organization, and due to the sensitive nature of the data connected to HR requests, we ensure that only authorized HR personnel are able to access such sensitive, personal information. Even the IT system administrators do not have authorization to access the data in the HR application.

HR departments typically use multiple systems and applications to manage core HR, benefits, payroll, recruiting, talent management, employee documents, and employee communications – sometimes all separately. Secure integrations into these existing systems are vital. ServiceNow 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 directly interact with its customers. Common requests, such as changes of personal details, password resets, and warranty registrations can be automated. Customers can browse service catalogue 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, it is essential that controls are in place to manage the identification, authentication, and authorization of users, while keeping public and private access separate at all times.

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

**Security operations product security considerations**

ServiceNow has a thorough understanding of security-based activities that are used to protect customers’ environments and data. ServiceNow performs these very same activities in securing both its private cloud and its own internal corporate environments. With the increasing rate and sophistication of attacks, it is more important than ever for organizations to manage the security of their environments effectively and efficiently.

The ServiceNow security operations application integrates with many of the commercially available security tools customers already use and augments these tools to apply business service mapping and workflow automation. Most responsible organizations undertake security incident response, vulnerability management, threat intelligence, or governance risk and compliance (GRC) programs.

These activities are essential components of a comprehensive approach to security and by their nature, 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.

**Data considerations**

**Data roles and responsibilities**

In data terms, there are two defined roles, each with its own associated responsibilities. In the case of a customer using ServiceNow, 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

There are also 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

As the data controller, the customer is responsible for determining how data is collected, stored, used, shared, archived, and destroyed, 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

Data processor

As the data processor, ServiceNow supports the 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

ServiceNow offers cooperation and assistance to data controllers in ensuring compliance with data controllers’ obligations pursuant to applicable data protection laws. For more details, see ServiceNow’s 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 data center (DC) pairs, where both members are either within the same jurisdiction or within mutually compatible jurisdictions so that even when data is transferred from one DC to another, the sovereignty of the data is preserved.

The storing and hosting of data are two distinct concepts, and ServiceNow only hosts customer data. Figuratively, ServiceNow provides a box and secures it (hosting), whereas customers decide what they put into the box (storing) and who can access it.

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. The Now Platform provides the capabilities to:

- Authenticate users before access
- Encrypt passwords
- Allow users to manage passwords
- Prevent access by users with an inactive account

ServiceNow maintains sufficient controls to meet the objectives stated in ISO 27001, ISO 27018, SSAE18/SOC 1 and SOC 2 Type 2 (or equivalent standards) 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 maintains a document repository called CORE to conduct data protection impact analysis (DPIA), if necessary.

In addition to our security measures, customers also have a share of responsibility in protecting their data, which includes:

- Managing each user’s access to (and use of) the service
- Implementing encryption and/or access control functionalities that are available within the subscription service
- Protecting the confidentiality of each user’s login and password

**Data privacy operations**

Data subjects have basic rights to privacy. The responsibility for upholding and supporting these rights is shared between the data controller and data processor. The GDPR is currently the highest standard of data privacy regulation globally, so GDPR is a useful benchmark for operations related to data privacy.

ServiceNow provides data controllers with the ability to access, correct, rectify, erase or block personal data – or 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 (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. ServiceNow 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.</td>
</tr>
<tr>
<td>Right of access</td>
<td>Data subjects may request information regarding their personal data from the data controller 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 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>Individual’s rights</td>
<td>Description and how ServiceNow supports these rights</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 data controllers 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. Data controllers are fully responsible for the erasure of data. ServiceNow has comprehensive auditing and reporting features which 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 in which 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 aged over a period of 28 days 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.</td>
</tr>
<tr>
<td>Right to restrict processing</td>
<td>Data subjects may request that certain processing is blocked. This is a wide-reaching topic which may involve many variables. ServiceNow has a flexible database and business rules system which allows easy tagging of individual records and conditional processing (i.e. respecting a &quot;do not share&quot; restriction and reporting on such activities or restrictions). These activities are the responsibility of the data controller.</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 the common open CSV format, XML, JSON, etc. The ability to extract data in a variety of forms is a built-in feature supported universally throughout the platform, allowing data controllers to easily comply with this requirement. These activities are entirely the responsibility of the data controller.</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. ServiceNow can be used to automate and record this. These activities are entirely the responsibility of the data controller.</td>
</tr>
</tbody>
</table>
Individual's rights | Description and how ServiceNow supports these rights
--- | ---
Rights related to automated decision making and profiling | These rights introduce safeguards against the risk of a potentially damaging decision being taken without human intervention. ServiceNow’s comprehensive workflow engine allows for comments, approvals, conditional processing, and multi-channel integration with human decision makers. This allows data controllers to build processes that comply with this right, and 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.

Data return and destruction
Throughout the lifetime of the subscription, data can be directly exported using features available in a ServiceNow instance. This can be via the UI interface through integrations or by using optional ServiceNow components, such as the free ODBC connector or MID Server.

Upon contract expiration or exit, or where requested, ServiceNow will supply a customer’s data in an SQL dump format. Exiting customers have 45 days to request their data to be returned, after which all hosted and backed-up data is automatically deleted and overwritten.

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.

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 ServiceNow, 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 ServiceNow’s service mapping function, and vulnerability response application.

Storing CMDB data and related information in the cloud
A common concern over storing asset 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. So 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.

ServiceNow orchestration and discovery
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 in order to operate entirely within their infrastructure.
As with any other enterprise endpoint deployed by a customer, MID server activities can be limited using network and administrative controls, including credential management systems. MID servers run commands generated on the ServiceNow instance by appropriately credentialed customer administrators and then placed in a fully auditable event queue that 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 them.

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.

Data used for machine learning and artificial intelligence

Data used for machine learning

Training and prediction data never leaves the data center (DC) and is transferred between instances and their local dedicated machine learning (ML) servers over HTTPS. Customers determine what data is sent to the ML trainer when they define what to learn, and the scope, e.g. the data from 6 months of closed tickets and short descriptions. These configurations are recorded and available for audit.

Once the system training is completed and a training model is returned to the requesting instance, the data and model are deleted from the training and prediction server. No human intervention occurs throughout the process.

ML is also used in natural learning understanding (NLU), which powers the virtual agent. NLU uses the same prediction infrastructure, but in this case, customers create models of ‘intents’ along with associated ‘utterances’ (e.g. voice commands to open a ticket). No customer data is used other than the utterances themselves.

The DART program (Data Access for Responsible Training)

ServiceNow has introduced the DART program to help accelerate and refine the development of Now Intelligence. This brings the benefits of automation, anomaly detection and prediction to the platform, improving the customer experience and resulting in a faster time to resolution.

Features such as artificial intelligence (AI), natural language understanding (NLU), and machine learning (ML) must be tested and optimized during development. This is most effectively done using real–rather than synthetic–datasets. The DART program enables ServiceNow to test Now intelligence algorithms against data stored in temporary clones of customer instances.

Customers are automatically enrolled into the program when their contracts are renewed but retain complete control over the use of their data and are free to start, pause, or stop their participation at any time. Customers’ DART clone is deleted when they leave the program.

DART clones and the associated Now intelligence infrastructure are all deployed within a carefully controlled, isolated, and secure environment. Only a select, authorized, subset of ServiceNow employees can access the environment – and only from company–provisioned devices via VPNs that are authenticated by multifactor authentication (MFA). It is not possible for DART clones and infrastructure to connect to other instances or to the Internet. There is no data commingling, and the clones are not backed up.

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 customer support tickets.

ServiceNow access to customer data

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

Only members of ServiceNow’s 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 gained 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 Data Access Controls.

Technical controls

Overview of authentication and authorization

Customers can integrate their Now Platform instances with existing authentication services if required, including those that use directory or single sign-on (SSO) technologies, such as LDAP or SAML. This means that user accounts can be managed within the customers’ existing processes and standards. Alternatively, customers can define roles and groups within the instance itself.

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. The attributes that are available vary with the type of object being secured. Customers have full 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

Most activities within an instance can be recorded in an audit log, and the Now Platform includes comprehensive access, event, and transaction logging.

The extent of logging is customer configurable, and detailed logging can be used to record and report on all activity within an instance. Logs can be reviewed directly within the ServiceNow instance or exported to a customer’s security information and event management (SIEM) tool. Workflows or incidents can be automatically created based upon 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.

ServiceNow collects and retains logs and events relevant to its entire cloud infrastructure, including information regarding requests made to instances of the Now Platform in order to detect potentially malicious actions or activities in relation to its service. ServiceNow uses such log and event management in conjunction 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 ServiceNow’s 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>
</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. The internet, however, is a public network and therefore communications can potentially be intercepted and read 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 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. This is also true of any data transferred from the on-premises MID server to the Now Platform. All end-user access to a ServiceNow instance attempted over HTTP are 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 are also able to use IP range-based authentication to restrict the public networks that are used to access their instances of the Now Platform.

The standard contractual clauses are applicable as a data transfer mechanism, as per section 9 (international data transfers) of ServiceNow’s 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 and the data processor, and who can access the data in an instance. It has also explored the security controls available to customers to enforce and audit this access and to protect their instance. Further information about how ServiceNow secures the Now Platform can be found in the [Securing the Now Platform eBook](https://www.service-now.com.ebook).