Safeguarding Your Data
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 that the data's confidentiality, integrity, and availability is protected 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.

This document discusses different types of data, how they are handled, and gives an overview of what controls ServiceNow provides to assist customers in keeping their data safe.

Roles and responsibilities

Roles

In data terms, there are two defined roles: data controller and data processor, each with their own associated responsibilities.

- 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.

In the case of a customer using ServiceNow, the customer is the data controller, and ServiceNow is the data processor.

There are also terms applicable to data privacy that will be discussed later in this document:

- 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.

Responsibilities

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.

As the data processor, ServiceNow supports the controller by providing features for 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.
Data controller (customer)  
Has wider legal obligations and determines:

Data processor (ServiceNow)  
Has accountability obligations:

<table>
<thead>
<tr>
<th>The purpose of collecting the data</th>
<th>Supports the controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>What data is collected</td>
<td>Processes data on behalf of the controller</td>
</tr>
<tr>
<td>How the data is used</td>
<td>Ensures confidentiality</td>
</tr>
<tr>
<td>How long the data is retained</td>
<td>Ensures technical and administrative measures are in place to protect the data</td>
</tr>
<tr>
<td>Where the data is stored</td>
<td>Enables the keeping of data processing records</td>
</tr>
<tr>
<td>Who the data processor is</td>
<td>Informs the controller of any data breaches</td>
</tr>
</tbody>
</table>

Data sovereignty

Data is subject to the laws in 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.
Personal data

What is data privacy?

Data privacy addresses the rights of an individual over personal data held about them. This type of information is often subject to strict regulation. Personally identifiable information (PII) is any information that relates to a living person, such as name, date and 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, criminal record, etc. 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 can’t 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.

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 this document refers to GDPR as a benchmark for operations relating to data privacy.

All data regarding individuals must have a lawful basis for processing, which is determined by the data controller, and individuals have rights as defined below:

<table>
<thead>
<tr>
<th>Individual’s right</th>
<th>ServiceNow process or feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to be informed</td>
<td>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>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>Individual’s right</td>
<td>ServiceNow process or feature</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------</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. This is the data controller’s responsibility. 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 “do not share” 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>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.</td>
</tr>
<tr>
<td>Right to object</td>
<td>Individuals 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>
<tr>
<td>Rights related to automated decision making and profiling</td>
<td>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.</td>
</tr>
</tbody>
</table>
Asset data

Managing asset data

Asset data refers to both direct and related information about an asset (e.g. details of a PC), security event data, vulnerability information, and stored credentials for discovery and orchestration, among other 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, or 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 asset data in the cloud

CMDB data and related information

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 infrastructure. These risks are often overstated, since access to the internal network is required before the data can be used. A skilled attacker 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. To this end, 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 the Securing the Now Platform eBook.

ServiceNow orchestration and discovery

ServiceNow Management, Instrumentation and Discovery (MID) servers allow controlled communication between customer Instances and their internal network services and operate entirely within customer infrastructure. As with any other enterprise endpoint, 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 administrators and then placed in an 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 them. All event queue actions are fullyauditable.

Events are retrieved every 15 seconds via a secure TLS channel between the MID server and its 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

Customers who take advantage of the machine learning (ML) capabilities in the Now Platform may have concerns about the security of ML data.

ML uses dedicated training/prediction servers located in each data center. These servers may run multiple instances of the training/prediction application, but only serve the instances within that data center. Training/prediction servers are architected for high availability, but the data is not backed up. Training data from only one instance is processed on a trainer at any time and needs no human intervention. It is deleted once the system training is completed.

The customer decides what is to be learned, and therefore determines what data is sent to the ML trainer. They define the scope of the data, e.g. 12 months of tickets and short descriptions. Data is transferred from instances to the ML servers over HTTPS and with customer-specific authentication.

ML is also used in Natural Language 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. In this use case, no customer data is used other than the utterances themselves.
Who can access customer 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 in order to provide support. This is done on an incidental, per event basis, and not every customer support event will require access to customer data. Access to a customer’s instance where absolutely necessary takes place via a strictly controlled process.

Only members of ServiceNow’s support organization that 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 VPN that requires two-factor authentication, initiated from a physical ServiceNow owned device, which has a ServiceNow digital certificate installed.

Once authorized, these employees are only able to access the infrastructure via a highly restricted virtual environment. This provides a secure sandbox in which they are able to undertake their duties. All such activities are logged in detail and immediately visible to customers within their instance and also within the Now Platform® infrastructure, which is under constant scrutiny from a dedicated security operations team. More information can be found in the Data Access Controls white paper available on ServiceNow CORE.

Technical controls

Authentication and authorization
Customers can integrate their existing authentication services if required, including those which 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.

After authentication, the Now Platform’s role-based access control system (RBAC) allows customers to control access to the 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 granted to each of their users and integration with directory services is possible with users, groups and group memberships.
Auditing and logging

Most activities within an instance can be recorded in an audit log, and the Now Platform includes extremely 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 historical 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.

<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>Import</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

Customers access the Now Platform via a web browser. All data is transferred exclusively over HTTPS, meaning that the data-in-transit is encrypted. This is also true of any data transferred from the on-premises MID server to the Now Platform.

Customers are also able to use IP range-based authentication to restrict the public networks used to access their instances of the Now Platform for additional security. This is set to default ‘deny’ and only allows specified whitelisted IP addresses to access the instance.

Email encryption allows emails and attachments to be encrypted while in transit to and from the instance using TLS encryption.
Encryption

ServiceNow also offers its customers several encryption options intended to address additional data protection and privacy needs for at-rest data.

Column encryption of customer-added fields and attachments provides encryption via AES-128/256. The keys for this encryption are provided by the customer and stored in the relevant instance database in an encrypted form, using a “wrapper”, or key encrypting key, stored in a separate key management appliance.

Database encryption, an additional cost option, enables all stored data to be encrypted via AES-128 while the database is operational, and the instance is in use. Individual tables are decrypted only when accessed, and any new or changed data is encrypted as it is entered. This process is completely transparent to users – they continue to work as normal – and there is no loss of functionality. When this feature is enabled, encryption is applied to all of a customer’s instances, along with replication traffic and backups. Encryption keys are protected by a three-tier encryption model, utilizing a management appliance.

Edge Encryption, another additional cost option, allows customers to create and control their encryption keys within their own network. Edge Encryption includes a proxy application that resides in a customer’s network and acts as a built-in cloud application security broker (CASB). This encrypts or tokenizes data before it is sent from the customer’s environment to the ServiceNow instance. The data always remains encrypted while stored in the instance, and the data, keys, and encryption configuration are never accessible by ServiceNow.

Full disk encryption, also an additional cost option, is provided via self-encrypting hard drives with 256-bit AES encryption and is transparent to an instance of ServiceNow where deployed. This encryption can only be used with dedicated hardware and is focused on preventing data exposure in the unlikely event of loss or theft of the physical disks hosting customer data.

These options are explored in more detail in the ServiceNow Encryption Technical Summary and the Data Encryption eBook.

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.