Understanding Your Data

The ServiceNow Trust Journey
Our commitment to security

At ServiceNow we believe it is our duty to ensure that every customer has complete confidence in our commitment to safeguarding the security of their data assets.

We build security into the Now Platform® and our products from the ground up to make sure that we effectively safeguard the confidentiality, integrity, and availability of all our customers’ information—a mission we take very seriously.

This document is part of a journey designed to assist our customers, both new and existing, in understanding the strong measures that we have in place to ensure that all data processed on our platform is safe and secure.

We speak your language

At ServiceNow we take great pride in a providing a market-leading platform that enables business to work more efficiently and effectively. We believe that in order to provide industry-leading security for our platform, it is essential that we understand the data security needs and concerns associated with your use case. Each product line listed below has different requirements; please read those which are applicable to you.

**IT Service Management (ITSM)**

ITSM departments handle large quantities of data daily. This data is stored in the configuration management database (CMDB) and includes requests related to incidents, problems, and changes, such as password resets, computer hardware issues, patch management, and maintenance.

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. This key configuration data could be 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. This data is broadly classified as asset data and is discussed in the document ‘Safeguarding Your Data’.

**IT Operations Management (ITOM)**

ITOM activities handle large quantities of data daily. Critically, this data may include user credentials, so protecting these assets is essential to the security of the organization as a whole.

It is also important that communication with ServiceNow 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.

ITOM is a key business application upon which ServiceNow has developed a range of product offerings, all integrated with the entire ServiceNow solution. ServiceNow is a leader in this industry, and as such, understands the data privacy and security concerns associated with corporate asset data in great detail.

As with ITSM, data assets stored in the configuration management database (CMDB) could be 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. As an organization that relies on complete mastery of its
own technology, ServiceNow understands how critical this data is, and how tough those protections must be.

This data is stored in the CMDB and contains detailed information about IT-related assets, such as server models, OS versions, patch levels, dependencies, and IP addresses. This data is broadly classified as asset data and is discussed in the document ‘Safeguarding Your Data’.

**IT Business Management (ITBM)**

ITBM involves financial, strategic, and resourcing information. As such, maintaining accurate data, connecting business users, assets, processes, and more—and securing all aspects of that integration—is essential. Collecting user-generated, free-form information can sometimes result in the inclusion of additional unnecessary, sensitive data. When this occurs, that information must be identified and protected, and may need to be handled differently.

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

The document ‘Safeguarding Your Data’ details the controls in place to assist in managing the challenges of asset and personal data.

**Human Resources (HR)**

The HR industry keeps a wide variety of personal data that is of a highly sensitive nature, from ID numbers to copies of passports, disciplinary data, or medical history. Employees also confide in the HR department when it comes to personal matters, including mental health and work/life balance. In fact, it is hard to imagine a department that handles more personal and sensitive data than HR, and it is easy to see why safeguarding that data is of paramount importance.

ServiceNow believes that 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.

It is precisely this attention to detail that allows the many global customers of our HR offering to entrust their most sensitive data assets to ServiceNow, and they have done so safely and securely.

ServiceNow also recognizes that 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. The importance of secure integrations into these existing systems cannot be overstated. ServiceNow currently supports a wide range of integration methods with third-party HR applications.

Any compromise of the confidentiality, integrity, and availability of HR information could have severe consequences including regulatory, professional, identity, and company reputational damage.

Information security best practice rightly acknowledges the importance of this data and of protecting it effectively, both when it is stored (at rest) and transported (in transit). To information assurance and data privacy professionals, HR data falls predominantly into two categories: personally identifiable information (PII) and sensitive personal information (SPI).

PII is data which relates to a living individual who can be identified by that data. SPI is an extension of that, which is subject to strict regulation and includes ethnic origin, political opinions, health information, criminal record, etc.

However, while there are differences in the way PII and SPI are classified by organizations and which information falls into each type, in data terms they are all treated the same and have to comply with the same regulations and safeguards. These terms are discussed further in the document ‘Safeguarding Your Data’.
Customer Service Management (CSM)

ServiceNow offers a powerful CSM application that 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 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, we understand that 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 ServiceNow 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.

Information security best practice rightly acknowledges the importance of this data and of protecting it effectively, both when it is stored (at rest) and transported (in transit). To information assurance and data privacy professionals, CSM data falls predominantly into two categories: personally identifiable information (PII) and sensitive personal information (SPI).

PII is data which relates to a living individual who can be identified by that data. SPI is an extension of that, which is subject to strict regulation and includes ethnic origin, political opinions, health information, criminal record, etc.

However, while there are differences in the way PII and SPI are classified by organizations and which information falls into each type, in data terms they are all treated the same and have to comply with the same regulations and safeguards. These terms are discussed further in the document ‘Safeguarding Your Data’.

Security Operations

ServiceNow has a deep understanding of security-based activities that are used to protect customers’ environments and data. After all, 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 effectively and efficiently manage the security of their environments.

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, just as we do ourselves.

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. This data is broadly classified as asset data and is discussed in the document ‘Safeguarding Your Data’.

Continuing the Trust Journey

The next stage in the Trust Journey, the document ‘Safeguarding Your Data’, looks in more detail at the challenges associated with asset data and expands on PII/SPI. This document discusses the different roles of the data controller and the data processor and the controls at your disposal to protect the confidentiality, integrity, and availability of the data you process with ServiceNow.