Whitepaper
2018

Watson AI Privacy, Compliance & Security

IBM

Table of Contents

"Every organization that develops or uses AI, or hosts or processes data, must do so responsibly and transparently. Companies are being judged not just by how we use data, but by whether we are trusted stewards of other people's data. Society will decide which companies it trusts."

Ginni Rometty, IBM Chairman, President and CEO

Introduction

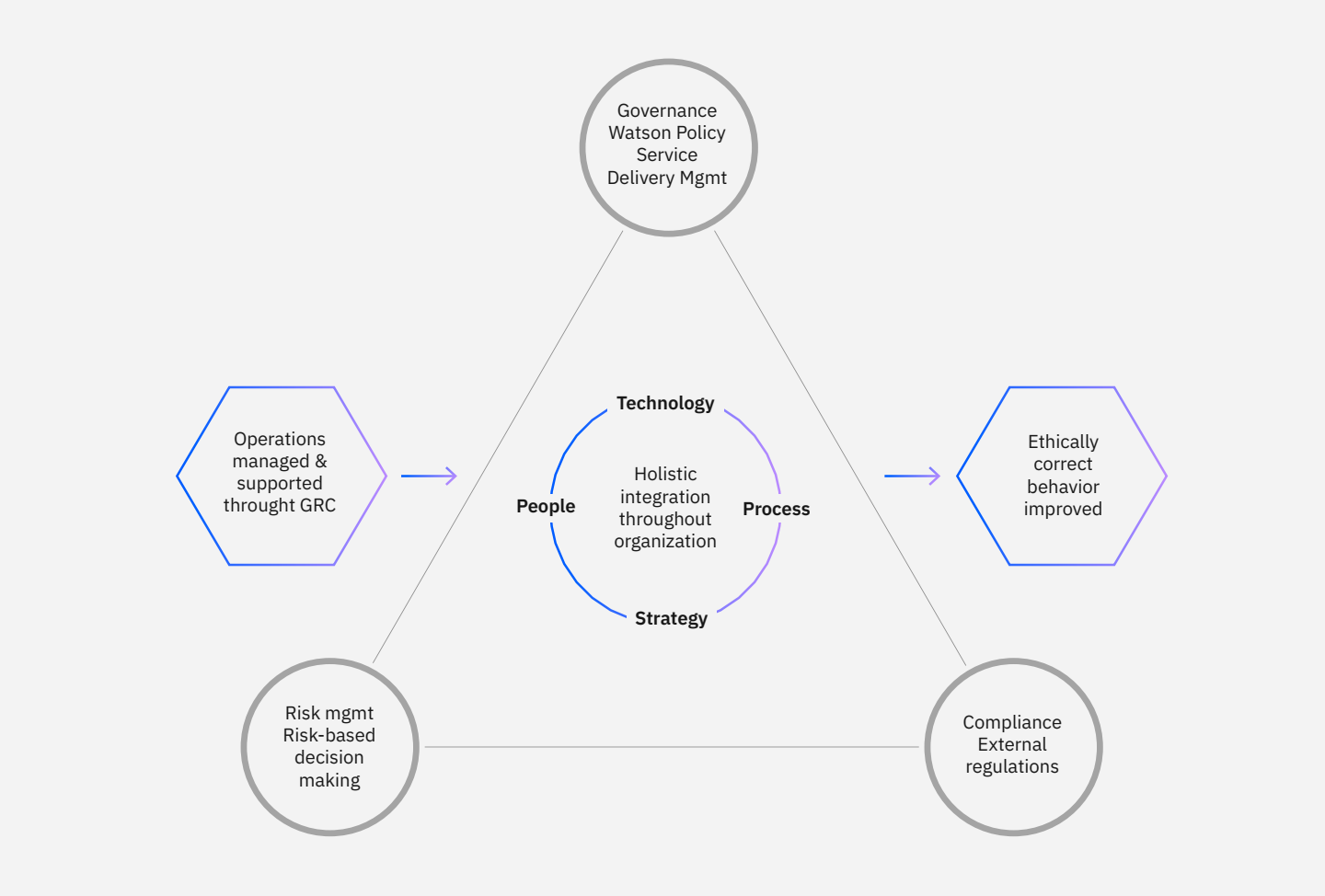
The ability of artificial intelligence (AI) to transform vast amounts of complex, ambiguous information into insights has the potential to reveal long-held secrets and solve some of the world's most enduring problems. It can help us cure disease, predict the weather, and manage the global economy. It is an undeniably powerful tool. And like all powerful tools, great care must be taken in its development and deployment.

To reap the societal benefits of artificial intelligence, we will first need to trust it. We have created a system of best practices that guide the safe and ethical management of Watson (IBM's leading AI computing capabilities); a system that includes contracts and disclosures that help foster full transparency; a strategy that reflects our compliance with existing legislation and policy; and a framework that protects privacy and personal data.

IBM uses robust security and compliance processes that allow for successful execution of challenging workloads. The IBM Secure Engineering Framework reflects best practice from across the company and directs our development teams to give proper attention to security during the development lifecycle. These practices are intended to help enhance product security, protect IBM intellectual property and support the terms of warranty of IBM products. Secure Engineering is an important element of the overall IBM security strategy. It is reflected in our internal initiative that addresses the dynamic nature of security in our development process. It is also reflected in our drive to meet the demand for high quality, high assurance business solutions, services and Information Technologies for our customers and our own operation.

This document describes the Security, Data Privacy, and Compliance policies of the Watson AI services running on IBM Cloud. The document does not address other IBM or client offerings with Watson in their name (e.g., Watson Health), or services that are not in the Watson part of the IBM Cloud catalog. Nor does it address any third-party services showing up under Watson in the IBM Catalog.

Structures of compliance strategy



The IBM Watson data compliance strategy is built upon industry Governance, Risk, and Compliance (GRC) principles shown above, with compliance certifications as a key part of IBM's ongoing commitment to providing a secure platform for business. This Watson on IBM Cloud security site provides further details.

"Your data is yours, not mine to give away. If it's artificial intelligence, you own the insights, you own the algorithms."

Ginni Rometty, Chairman, President, and CEO, IBM
Dreamforce 2017, San Francisco, CA, November 8, 2017

Data privacy

What is it?
Protect your insights. Data is an organization's most valuable asset. It can yield unique competitive advantage coupled with the power of AI. But as data— and the models you build with it—become more and more valuable, you need to ensure you have control and choice over how it's used. When you train Watson with your data, your data and your insights are for your use only. But across the spectrum of data businesses generate, some models may gain more value if you decide to share with others whose innovations may accrue back to you.

At IBM we believe your data is yours – and yours alone. Therefore, it's essential to create a system of best practices that guide the safe management of data, including IBM Watson services and the data Watson is trained on. This includes contracts and disclosures that help foster full transparency; a strategy that reflects our compliance with existing legislation and policy; and a framework that protects privacy and personal data.

Prove it
IBM will not share unique insights derived from your data without your agreement. You are also not required to relinquish rights to your data in order to have the benefits of Watson services. Watson Standard clients may opt-out of letting Watson use their data beyond for their own use. For Watson Premium and Dedicated clients, opt-out is the default setting. When you use Watson services on the IBM Cloud, you will have the ability to combine your data sets with other IBM-owned, licensed, or public data sets to yield broader insights.

The Cloud Service Data Security and Privacy site has data sheets for each Watson AI service. The data sheet for each service discusses the types of personal information used, processing activities, data protection, removal of the data at termination of the service or by request, data hosting locations, international data transfer, and more.

IBM makes clear when and for what purposes your data is being applied in the solutions we develop and deploy. This may include the major sources of data and expertise that inform the insights of AI solutions we develop. Third-party or licensed data will be clearly identified.
IBM agreements are transparent. We will not use your data unless you consent to such use, and then we will limit that use to the specific cases clearly described in the agreement. In addition, IBM will not share unique insights derived from your data without your agreement. IBM will remove client content at the request of a client or at the end of the cloud service.

Because all Watson AI services have received ISO 27018 Certification, Personally Identifiable Information (PII) can be accepted by Watson AI services in the Standard, Premium, and Dedicated deployment options, with the exception of regulated data types such as Personal Health Information (PHI) (e.g. HIPAA), and Payment Card Industry (PCI) data, which have separate certification recommendations.

Each Watson AI service SLA includes a link to a data sheet which provides details on how security and data privacy is provided for that service. The Cloud Services Data Security and Privacy site has the data sheet for each service.

IBM makes clear when and for what purposes your data is being applied in the solutions we develop and deploy. This may include the major sources of data and expertise that inform the insights of AI solutions we develop. Third-party or licensed data will be clearly identified.

IBM agreements are transparent. We will not use your data unless you consent to such use, and then we will limit that use to the specific cases clearly described in the agreement. In addition, IBM will not share unique insights derived from your data without your agreement. IBM will remove client content at the request of a client or at the end of the cloud service.

Because all Watson AI services have received ISO 27018 Certification, Personally Identifiable Information (PII) can be accepted by Watson AI services in the Standard, Premium, and Dedicated deployment options, with the exception of regulated data types such as Personal Health Information (PHI) (e.g. HIPAA), and Payment Card Industry (PCI) data, which have

For more details
Read more on cloud privacy

Watson AI privacy policies
Click to read

Other resources
Click to read

Compliance and regulation

What is it?
As a business, it is your responsibility to protect your customers' data. It is imperative that the cloud provider you choose to be in compliance with relevant standards. The provider must place a premium on security, and transparency in how they will use the data you share. After all, if your customers' data is compromised, your company will be blamed. You will only maintain the trust of your customers by being proactive in keeping their data safe.

To choose a cloud provider that meets the required compliance standards, you must understand the types of data you have because different types of data have their own compliance standards. Compliance standards exist for many industries and may vary by country or region. Here are several examples.

- If you store health information for U.S. patients, U.S. Health Insurance Portability and Accountability Act (HIPAA) compliance is important
- If your data pertains to residents of the European Union, then General Data Protection Regulation (GDPR) compliance is critical
- To ensure consistent standards for merchants, the Payment Card Industry Security Standards Council established Payment Card Industry (PCI) data security standards

Prove it
IBM Cloud's compliance and trust certifications are another confirmation of our strong commitment to protecting your data and your cloud. You can be confident that when it comes to meeting the world's global and regulated industry standards, we've done the work for you.

Check out the IBM Cloud compliance page for more details on IBM Cloud compliance. See the table below for details on Watson AI services.

The Cloud Security Alliance CSA is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within cloud computing. One of the mechanisms the CSA uses in pursuit of its mission is the Security, Trust and Assurance Registry (STAR) — a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings. For those looking for detailed answers to specific cloud security questions, the CSA assessment is an excellent source of answers. IBM Cloud's CSA STARS CAIQ assessment is here. Scroll down on that site, you will see the Watson AI self-assessment.

EU Model Clauses are available to controllers and processors of EU citizens' Personally Identifiable Information (PII). These clauses obligate non-EU companies to follow the laws and practices mandated by the EU in all global locations. The clauses provide enforcement rights and comfort to companies holding EU PII , stipulating that providers located outside of the EU will process data only in accordance with their instructions and in conformance with EU laws. Watson AI services are compliant with the EU Model Clauses. The clauses provide enforcement rights and comfort to companies that hold EU PII that providers located outside of the EU will process data only in accordance with their instructions and in conformance with EU laws. EU Model Clauses in place for the Watson AI services - here. Note that even with GDPR, there is still a place for EU Model Clauses. These are all methods of international data transfer, which GDPR needs to be under sufficient international control.

GDPR Compliance regulation

Compliance Standard	Compliance for both IBM Cloud & Watson AI services	Watson Standard	Watson Premium
ISO27001	ISO 27001 is a widely adopted global security standard outlining the requirements for information-security management systems and provides a systematic approach to managing company and customer information based on periodic risk assessments. ISO 27001 certificate Full list of IBM products covered under 27001	Yes	Yes
ISO 27017	ISO 27017 gives guidelines for information-security controls applicable to the provisioning and use of cloud services, as well as implementation guidance for both cloud service providers and cloud service customers. ISO 27017 certificate	Yes	Yes
ISO 27018	ISO 27018 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO 29100 for the public cloud computing environment. ISO 27018 certificate	Yes	Yes

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU. See this site documenting IBM's commitment to GDPR and IBM's Journey to GDPR Readiness eBook. The three Watson AI deployment models above are GDPR-ready.

Security

What is it?
The growth of cloud and mobile computing and Internet of Things (IoT) technologies is accelerating the shift in IT services away from "on-premises" towards cloud. Every member of your company, every device, and every piece of software is vulnerable to attacks, for which your leadership will be held accountable – especially if they chose the wrong cloud provider. Your data security and privacy considerations are only as strong as those of your cloud provider, so it is critical to choose a provider that is both secure and transparent with their security processes. The provider must be able to detect and react to threats, as well as proactively take actions to prevent them from occurring in the first place.

The Oracle and KPMG Cloud Threat Report 2018 offers these sobering observations:

- Some 90% of businesses in a new survey say that at least half of their cloud-based data is indeed sensitive – the kind that cybercriminals would love to get their hands on
- 66% of companies in the study say at least one cybersecurity incident has disrupted their operations within the past two years
- 80% say they're concerned about the threat that cybercriminals pose to their data
- 20% of respondents to the survey say the cloud is much more secure than their on-premises environments; 42% say the cloud is somewhat more secure; and 21% say the cloud is equally secure; only 21% think the cloud is less secure
- 14% say that more than half of their data is in the cloud already, and 46% say that between a quarter and half of their data is in the cloud
- That cloud-based data is increasingly "sensitive," the survey respondents say. That data includes information collected from customer relationship management systems, personally identifiable information (PII), payment card data, legal documents, product designs, source code, and other types of intellectual property

Prove it
In the era of ever-present attacks and breaches, IBM Cloud Security's scalable suite of technologies and solutions are made more robust and complete through pervasive encryption, AI with automation and integration. When you partner with IBM, you gain access not only to a full stack of IBM Cloud security services, but also to an IBM security team supporting more than 12,000 customers in 133 countries.

No matter which IBM Cloud service you subscribe to, you can rest easier knowing that your content is protected by IBM's world-renowned security leadership. Every IBM Cloud service is designed, developed and managed according to IBM's own strict security policies and implementation guidelines, and provided to you under the commitments of the IBM Data Security and Privacy Principles.

Watson AI services on the IBM Cloud help to transform businesses enhancing competitive advantage and disrupting industries by unlocking the potential within unstructured data. Fundamental to providing a strong foundation for companies wanting to leverage Watson services, IBM uses robust security and compliance processes that allow for execution of challenging workloads.

IBM employs robust security procedures to safeguard the data with which Watson interacts. This includes use of encryption, access control methodologies, and proprietary consent management modules, which allow us to code or move data to restrict access to authorized users and to de-identify and use data in accordance with applicable permissions.

The security policy for Watson AI services requires that all services include network and storage encryption, circuit and application level firewalls, security information and event management, intrusion detection, application source code scanning, third-party penetration testing, and regular vulnerability scanning.

Watson AI services are governed by the IBM Cloud Services data security and privacy principles. The technical and organizational measures apply to IBM Cloud, including any underlying applications, platforms, and infrastructure components operated and managed by IBM. See the Cloud Service Data Security and Privacy site for data sheets on the individual IBM Cloud services. The data sheet for each service discusses the types of personal information used, processing activities, data protection, removal of the data at termination of the service or by request, data hosting locations, international data transfer, and more.

IBM Watson has a policy of end-to-end encryption and employs the latest cryptographic technologies to protect client data. The IBM platform ensures:

- That end-to-end security for data in transit is implemented using TLS Version 1.2
- An optional mutual authentication certificate and/or user name and password for added measure via mutually authenticated SSL
- That data in transit and at rest is secured using AES 256-bit encryption

Additional security resources

- IBM Watson on IBM Cloud Security Overview - This site goes into detail on how IBM Watson provides security on the IBM Cloud. Encryption, network security, authentication, authorization, and more are topics covered.
- IBM Watson Data Perspective - Provides the IBM Data Responsibility Perspective for Watson Data and AI.
- IBM Cloud Services data security and privacy principles - This site has documents related to data security & privacy for IBM Cloud Services offerings.
- Cloud Services data security and privacy - This site describes overarching policies and practices that are incorporated into each service description by reference.
- IBM Charter of Trust for Cybersecurity - This February 16, 2018 blog describes the Charter of Trust for a secure digital world. Launched at the Munich Security Conference, this Charter established 10 key cybersecurity principles that IBM, Siemens, Airbus, Allianz, Daimler and others are adopting to strengthen trust in the security of the digital economy.
- IBM Principles for Trust & Transparency - Describes how Data Responsibility and Privacy is handled for AI.
- IBM Cloud Security - This site is part of the DOCS associated with IBM Cloud. Note that this site also links to the IBM Cloud Security architecture.

Resources on AI Bias

- THINK Policy Blog- Bias in AI: How we Build Fair AI Systems and Less-Biased Humans
- White paper - Mitigating Bias in AI Models by Ruchir Puri
- THINK 2018 conference 5 in 5 presentation, Las Vegas - Unbiased AI, Francesca Rossi

---

For more details on the IBM Cloud Security Policies
Click to explore

Frequently asked questions

Data Privacy

1. How does IBM Cloud and Watson handle PII, including regulated PII like health and credit card information?

IBM Cloud can handle non-regulated personally identifiable information (PII), or sensitive personal information (SPI), in accordance with the ISO 27107 and 27108 standards.

2. Is Watson learning from my data? Does Watson train other client's models with my data if I opt-in?

The default for Watson Standard is that all client training data is used for continued development of the general models (opt-in). A client can opt-out on the transaction, service, or account level.

The general model could be used to build subsequent custom models.

The default for Watson Premium and Watson Dedicated is that no client training data is used for the development or enhancement of the general models or other clients' models (opt-out).

3. We hear the "your data is your data" message from all Cloud providers. Why is IBM different?

With the widespread use of social media, a common phrase regarding data privacy is "if you're not paying for the product, then you are the product". This is true for many search engines and social media platforms in wide use, and even the free apps you get in the Apple and Android app stores.

For more than a century, IBM has earned the trust of our clients by responsibly managing their most valuable data, and we have worked to earn the trust of society by ushering powerful new technologies into the world responsibly and with clear purpose. IBM has for decades followed core principles

– Grounded in commitments to trust and transparency – that guide its handling of client data and insights, and also its responsible development and deployment of new technologies, such as IBM Watson. See the IBM Principles for Trust & Transparency

4. Which Watson AI services are stateful, versus stateless?

A stateless service treats each request as an independent transaction that is unrelated to any previous request. A stateful service may store data to correlate a prior request with the request it is currently processing. The following Watson AI services are stateful:

– Discovery
– Knowledge Studio
– Language Translator
– Machine Learning
– Speech-to-Text for custom models; otherwise stateless
– Text-to-Speech for custom models; otherwise stateless

Compliance & Regulations

1. Which regulations do IBM Cloud & Watson AI services support? For example: PCI (credit cards), HIPAA (U.S. healthcare), FFIEC and FISC (financial), FISMA and FedRAMP (U.S. Federal). Country-specific directives like the NIS Directive, and GDPR (European Union)?

As of May 25, 2018, both Watson AI and IBM Cloud were GDPR-ready.

2. As a client, can I request your SOC 2 / SOC 3 reports, and CAIQ assessment?

A SOC 1 report focuses on controls at the service organization that would be useful to user entities and their auditors for planning a financial statement audit of the user entity and evaluating internal control over financial reporting at the user entity.

Request the SOC 1 and SOC 2 certificates through our customer portal (link resides outside ibm.com) or contact your IBM representative.

SOC 2 and SOC 3 reports focus on the service organization's system description and controls in accordance with specific criteria related to availability, security and confidentiality. SOC 2 includes auditor testing and results, while SOC 3 is a summary of the SOC 2 report that is available for public use.

– The SOC 3 report is on the IBM Cloud Compliance site.

The Cloud Security Alliance CSA (link resides outside ibm.com) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within cloud computing. One of the mechanisms the CSA uses in pursuit of its mission is the Security, Trust and Assurance Registry (STAR) — a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings.

– IBM Cloud's CSA STARS CAIQ assessment is here. Scroll down on the IBM Cloud Compliance site to see the Watson AI self-assessment

3. How does Watson use Privacy Shield, EU model Clauses, or Safe Harbor?

–Safe Harbor was used to govern the transfer of data between the EU and the United States. Safe Harbor was replaced with a choice of either Privacy Shield or EU Model Clauses

–IBM uses EU Model Clauses in contracts

– Now that Watson and IBM Cloud are GDPR-ready, paperwork has been submitted for Privacy Shield. The process should be complete by July 2018

4. How does Watson handle the "right to be forgotten" clause in GDPR?

Clients that require this control must label their data.

5. Is IBM Cloud certified for the following?

– ISO 20000-1 - Yes demonstrated with an ISO 27001 Certification

– SSAE 16 - Yes demonstrated with a SOC1 Type 1 or Type 2 report

– ISAE 3402 - Yes similar to SOC1, our auditors include this attestation as part of the SOC1 report

– EU Directive 95/46/EC - superseded by GDPR. IBM Cloud & Watson are GDPR-ready

– German Bundesdatenschutzgesetz (BDSG) - IBM Cloud IaaS is certified for the BSI C5 standard to meet the requirements. See https://www.trusted-cloud.de/en/standards

Security: Securing my data

1. How is access management handled?

See the Authentication & Authorization and Identity & Access Management sections in the IBM Watson on IBM Cloud Security Overview for details.

2. Do you provide fine-grained access management (e.g. edit rights to some, read rights to others)?

Users of a Watson service get an access key, but no levels of access are currently provided.

3. What do you offer a client that wants data isolation (e.g. for PHI)?

There are three deployment models: IBM Watson public cloud (Watson Standard), Premium plans that provide additional data isolation within the public cloud, or a Dedicated cloud environment if you need an infrastructure dedicated for your use only. Each environment offers the same service functionality and the security architecture remains consistent. All IBM deployments reside within hardened enterprise-class IBM Cloud data centers that are ISO27001 and SOC2 certified. See Securing Cognitive Apps in Watson on IBM Cloud Security for details behind the three Watson deployment models.

4.What are the different levels of isolation that I can get around storage and data?

There are three deployment models: IBM Watson public cloud (Watson Standard), Premium plans that provide additional data isolation within the public cloud, or a Dedicated cloud environment if you need an infrastructure that is dedicated for your use only. Watson Standard is multi-tenant. Watson Premium provides Data isolation, while Watson Dedicated provides further isolation through the tooling and service hardware. All three deployment models provide isolation. See Securing Cognitive Apps in Watson on IBM Cloud Security for details behind the Watson deployment models.

5. How can I tell when someone from IBM has touched my data?

Most of the Watson AI services are stateless, which means that Watson does not store partner data. See the earlier information regarding access trails for information on employee access. With EU model clauses, providers located outside of the EU will process EU PII data only in accordance with their instructions and in conformance with EU laws.

6. If Watson transfers my data to process it, how does Watson ensure it gets deleted (the verification processes)? Is this process auditable so I can know my data has been deleted?

Most of the Watson AI services are stateless, which means that Watson does not store partner data if a client "opts out". Audits are performed internally, but to protect the security and privacy of our clients, we don't share the processes.

7. How is data erasure handled when the client terminates their contract - either at the end of the contract or at any point before? How soon after the contract ends is the data erased? What proof can you offer that it was erased?

IBM will remove client content at request of client or at the end of the cloud service within 90 days after termination of the service. Some content will remain in backup until expiration of the backup.

- The following Watson AI services use one of the Compose databases for client data. Compose has a policy that data is stored for 120 days, and then it would be deleted at the end of a contract. IBM does not send out an e-mail to clients noting that their stored data was deleted
- Watson Speech services: Use Compose Postgres and RabbitMQ
- Watson Studio: Compose Redis, RabbitMQ, Postgres, etcd, and elastic search
- Watson Knowledge Studio: Uses Compose MongoDB
- Watson Discovery: Uses Compose Postgres, RabbitMQ, and Elasticsearch
- Watson Machine Language: Uses Compose RabbitMQ

8. Can I get a copy of my data sent to me - at contract end? At any time?

This is not an issue for stateless Watson AI services because your data is only on the platform transitorily. For stateful services like Watson Assistant and Watson Discovery, data a client sends to the service is sent by the client, used to train a model, and then deleted.

9. Can I keep my data local (on-premises) and yet still process it through the Watson services? In other words, connect to my data from the Cloud, but not transfer the data?

Your data needs to be transferred to the cloud to be processed by the Watson services. For stateless the data is only on the platform transitorily. For stateful services like Watson Assistant and Watson Discovery, data a client sends to the service is sent by the client, used to train a model, and then deleted.

10. What is your management system around data isolation that would lead to data privacy?

Watson AI services have three levels of data isolation: Standard, Premium, and Dedicated. See earlier descriptions of the three deployment models in earlier FAQs.

11. Does IBM allow a private, secure connection from the customer's data center to an IBM Cloud data center?

To get to a Watson AI service, a client would need an IBM Cloud Infrastructure (SoftLayer) account and use that network to establish a TLS encrypted connection.

12. How do the Watson AI services handle backup and recovery of my data?

- Data security goes beyond how we encrypt data that's being transferred. Clients want to know how often and when we backup data that's persisted in the IBM Cloud (for whatever reason)
- See the data sheets associated with each Watson AI service as well as the associated Service Descriptions which address backup and storage [Retention and Destruction] policies. As an example, here are links to the IBM Watson Discovery data sheet and IBM Watson Discovery Service Description

13. What insight do I have to your logs and processes? Can I get a log feed?

For the security and privacy of the IBM Cloud users, we don't share our logs with partners or clients. If information were required from the logs for a legitimate reason (such as an investigation), then IBM would work with the client to ensure that we shared the relevant information.

Security: Encryption

1. Do you provide encryption-at-rest and encryption-in-motion?

Yes. See the Encryption & Data Privacy section in the IBM Watson on IBM Cloud Security Overview for details.

2. What kinds of encryption do you handle, and when?

IBM Security Policy requires that all services include network and storage encryption. IBM employs the latest technically feasible cryptography technologies to protect customer data at rest and in motion. See the IBM Watson on IBM Cloud Security Overview for details.

3. How can I build a secure Watson application?

See How to secure your applications when using Watson services and Improve the effectiveness of your application security.

4. What is the management process around encryption keys: Access, alerts, audits, management?

See the Encryption & Data Protection, and Authentication & Authorization sections in the IBM Watson on IBM Cloud Security Overview for details. The is also information on Vulnerability Management.

5. Does IBM Cloud support Bring Your Own Key (BYOK) so I can supply the key for encryption-at-rest and encryption-in-motion?

IBM Cloud supports encryption-at-rest and encryption-in-motion. Currently, everything is encrypted using IBM managed keys. BYOK means customers can bring and manage their own encryption keys; this is currently targeted for later in 2018.

Security: Vulnerability Management

1. What is your vulnerability management process?

The IBM Product Security Incident Response Team (PSIRT) manages the security vulnerability management process, providing identification and remediation of security vulnerabilities. All IBM Watson services participate in this system. See the IBM Secure Engineering and Product Vulnerability Management site for detail.

2. What is the procedure in case of a data breach? How is the client notified and how soon after the breach? Where does IBM document the details of the breach? Can I get a Root Cause Analysis Report?

See the IBM Secure Engineering and Product Vulnerability Management site for details

Security Management

1. What is your health check posture for scanning devices and code for vulnerabilities? How often do you run the scan and how is remediation handled?

- See the Application Security sections in the IBM Watson on IBM Cloud Security Overview for details
- See Securing Cognitive Apps in Watson on IBM Cloud Security for details on the three Watson deployment models

2. When was your last penetration test? How often do you run the test? What are the results of the last test, as well as your remediation plan for any identified gaps?

- Penetration testing involves skilled practitioners using a wide array of automated tools and manual methods in an attempt to compromise a system. All services regularly undergo penetration testing, using both IBM teams and external vendors. Each service is tested at least annually by a certified external vendor. Different services are tested each quarter, as opposed to all IBM Cloud services being tested at once
- Any critical or high priority issues are addressed immediately, before any penetration test report is produced. IBM does not share the results of the penetration test with clients because making gaps public could expose the security and privacy of our clients. IBM will share an executive summary from the third-party report with clients or partners upon request

3. Am I allowed to conduct a walk-through one of your data centers to see how you handle physical security, badging, logs, etc.?

Clients and partners are not permitted to conduct a walk-through of an IBM Cloud data center. This is to protect the security and privacy of other clients using the IBM Cloud.

4. Can I see your ITS policy document? How did Watson and IBM Cloud do on the last audits?

Here are the Data Security and Privacy Principles for the IBM Cloud. This document is effectively IBM's ITS policy document for IBM Cloud. Any critical or high issues are addressed immediately, before the audit report is produced. IBM does not share the results of tests and audits with clients because making gaps public could expose the security and privacy of our clients.

5. What is your end-of-life policy for hardware in your cloud data centers (e.g. router no longer supported by vendor so no patches) as well as for software)?

Here is the end-of-life Management procedure for the IBM Cloud data centers

– Networking manages system's life cycles proactively with device manufacturers and/or vendors to remain compliant with FFIEC guidelines. The scope of our efforts is for device installation and maintenance only. While Networking does make decisions on which make and model to replace EOL devices, they must align with current architecture standards. Our procedures include:

- Maintaining an inventory of device model, manufacturer, and firmware version in IMS Tracking changes to the inventory of devices in IMS
- Proactively monitor manufacturer end-of-life product pages at a minimum of once per quarter
- Discussing aging devices regularly as part of business reviews with our vendors monthly
- Planning for the replacement of devices through our maintenance team

6. If I am a partner and sell my application to 100 clients, then I could have 100 instances on IBM Cloud Premium?

How can I get usage information for an individual client instance?

– You can see an individual offering's usage by going to: Manage -> Billing and Usage -> Usage. This will bring users to a dashboard for all of the instances of the offerings they've purchased, and the aggregated usage associated with them. By clicking 'View Instances,' users should be able to see granular details for the particular instances they are interested in

Are there capabilities to provide fine-grained security and authorization for a single instance?

– The partner's admin sets up instances, orgs, and spaces in IBM Cloud. They control the access for individual instances

How would a client know if a disgruntled employee deleted a production instance?

– This is an audit capability by API tied to fine-grained access. The information is logged, but the client has to call IBM Support to find the disgruntled employee's name

– If a disgruntled partner employee takes malicious actions, the partner could rotate or change the employee keys and then the disgruntled employee can do nothing further

If an instance goes down, how would the partner know?

– Either IBM Cloud will communicate that the service instance is down, or the partner will have to check the status page described earlier in this response

Watson Privacy, Compliance & Security

Whitepaper

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
July 2018

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The information in this document is provided “as is” without any warranty, express or implied, including without any warranties of merchantability, fitness for a particular purpose and any warranty or condition of non-infringement.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. **IBM does not warrant that systems and product are immune from the malicious or illegal conduct of an party.**