Mango

Maximum Security
Minimum Effort

Southwark
Greenwich
Tower Hamlets
Legend
Point Category Vertical with a very long title that wraps the line
Here is a descriptions that will be placed below the layer name.
Category 1
Category 2
Category 3
Category 4
Line Category Vertical
Here is a descriptions that will be placed below the layer name.
Category 1
Category 2
Category 3
MacBook Air

Mango

At Mango, the security of your data is our primary concern.

Who can see your datasets?

By default, all data uploaded to Mango is private.

Users of your maps do not have access to the underlying datasets. All data you upload remains private, accessible by the account owner, unless you specifically change dataset access permissions.

For Professional and Business plan users, raw datasets are only accessible to you, using your account credentials.

For Enterprise and Agency plan users utilizing add-on users, datasets will also be accessible to invited users whom you have specifically granted access via the Group access settings for each dataset.

Public datasets are available to view on your public portal by anyone, and can be downloaded as a geospatial file by anyone on the internet.

Mango staff do not have access to your raw datasets. Please see our Privacy Policy for further information.

Who can see your maps?

Maps are not accessible to anyone outside the account until they are switched online. Once online, external access to your maps is determined by each map's access settings.

Maps can be public, hidden, stand-alone, password protected, or internal.

Internal maps are only accessible to you, the account owner, and to invited users whom you have specifically granted access via the Group access settings for each map.

How is your data transferred?

All server requests to Mango are sent and received via SSL (secure socket layer) which uses a 256-bit encryption validated by GeoTrust.

GeoTrust®

How is your data stored?

Datasets uploaded to Mango are converted into an intermediary format that cannot be opened or read by desktop GIS packages.

Data uploaded to Mango is not accessible by or shared with any third parties.

What happens to your data when you delete a map or dataset?

When you delete a map or dataset from your account it is completely deleted from our servers and never stored for any kind of future use.

Where are your maps hosted?

Mango uses Amazon Web Services (AWS) for all infrastructure, with servers based in the US.

amazon web services

Map tiles generated from your data are cached and served via the AWS content delivery network with global distribution points to maximize delivery speed — no matter where you or your map users are located.

How reliable is Mango?

Mango benefits from the industry leading reliability of Amazon Web Services, and can boast 99.98% uptime thanks to resilient infrastructure and protocols. AWS adheres to more than a dozen US Assurance standards including FedRAMP, FERPA, FISMA, and NIST, and more than 50 global compliance audited certifications, regulations, privacy standards, and frameworks.

All of our servers are monitored 24/7/365. It doesn't matter if it's 3am on Sunday morning or Christmas Day, the moment a server experiences problems, alarms are activated on the cellphones of our on-call technicians.

What data redundancy protocols are in place to protect your data?

We take a snapshot of our servers daily and keep each snapshot for seven days. A snapshot isn't just a data backup — it's a complete copy of the server including the operating system and all data.

This means in the unlikely event of a critical failure we can instantly bring a complete copy of the server online.

Deliver optimal outcomes, maintain complete security.

As with most industries, GIS has a tendency to regard the Cloud with a certain amount of suspicion and trepidation—after all, it's simple for a GIS professional to deploy a single map containing all the public datasets, and keep private data private.

But does that provide the best outcome for the users of your maps and data?

For organizations that do publish maps for external users, the balance between open access and full lockdown is a choice that doesn't have to exist; instead, leveraging secure cloud services like Mango can deliver useful outcomes across all stakeholders and users.

Your organization's geospatial data is your most precious asset, and the thought of putting that data in cloud can raise a cold sweat.

It seems logical that it would be safer to keep data on premises. The physical proximity of desktops or servers are comforting, but what this inevitably leads to is siloed data and limited access for the users your data provides the most value to.

Migrating data from the back room to the front desk via the cloud utilizing elastic infrastructure provides efficient delivery outcomes that allows for increased visibility, analysis, and delivers greater value to a wider set of users.

Keeping sensitive data secure is a core necessity, but by holding out against the cloud just because some data needs to be restricted also restricts your open data that your users really do need.

Multi-tenancy cloud platforms, where many data stores share the same physical infrastructure, also raise the fear that data could inadvertently become exposed to others, including competitors.

Our infrastructure provider AWS is well aware of such concerns and have implemented layers of protection to ensure that you — and only you — have access to your data.

Mango's infrastructure maintenance procedures ensure applications and operating systems are patched and kept up to date, and employee access is secured with frequently changing root and administrator credentials, and multi-factor authentication including device specific sign in. Authentication keys are never stored in public repositories or in a manner which would allow for inadvertent publication.

Mango secures your data in a number of ways and provides granular access permissions that ensures only your authorized users have elevated access, and unauthenticated users only see what you have specifically made public.

Map data uploaded to Mango is not stored in its native format. It is converted into an intermediary format that cannot be opened or read by desktop GIS packages, further securing the data contained within.

Data uploaded to Mango is not accessible or shared with any third parties, and when you delete a dataset from your account it is completely deleted from our servers.

While Mango is built to secure your data, it's important to remember where your responsibilities lie, and how best to ensure that potential risk factors are mitigated and appropriate processes are built into your existing data security and governance policies.

Want to learn more about Mango's data security processes? Get in touch with our customer service team - simply send us a message when you are signed in to your account, or drop us a line: support@mangomap.com.

Mango

Security & Compliance

Robust security is critical for any organization, but a common complaint is that the cloud is simply not secure.

Cloud security, however, gains its strength from a seemingly inherent weakness—as a candidate for cyber-attack, the Cloud is an irresistable target.

With unprecedented amounts of data, users, attack vectors, and distribution of massive amounts of data to a wider geography than any single company or agency has managed before, cloud providers have amassed a wealth of security intelligence over the past few decades that has shaped real world security processes.

Today, these processes are without rival by any traditional means, and most certainly out of reach of small organizations.

In fact, existing in-house infrastructure may be the weakest point in your security processes.

It's not uncommon to find that physical security procedures for locally hosted servers is often neglected.

Consider how many people have had physical access to your locally hosted servers? You and your staff, but then what about cleaning staff, the site maintenance manager, his staff, third party contractors such as builders, pest control.

How many of these people have been vetted? How often do you review access authorizations?

The physical security of Amazon Web Services (AWS) cloud data centers exceeds traditional data center safeguards, and likely exceeds the capacities of most organizations

The core protocols of AWS physical security and protection includes:

- Background checks for all staff with physical/network access
- Review of staff credentials every 90-days
- Full audit log of all interactions with the servers
- Access Control/Intrusion Detection and CCTV Surveillance
- Fire detection and suppression
- Climate and temperature control
- Uninterrupted power supply systems and backup generators for the entire facility
- Storage device decommissioning processes that include degaussing and physical destruction

The IT infrastructure behind AWS is designed and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSÆ 16/ISÆ 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

In addition, the flexibility and control that the AWS platform provides allows Mango to meet several industry-specific standards, including:

- Criminal Justice Information Services(CJIS)
- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act(HIPAA)
- Motion Picture Association of America (MPAA)
- Secure Network Architecture / Secure Access Points
- Corporate Segregation (servers on a different physical network to staff)
- Fault Tolerant Design (one system gœs down a replacement gœs up)
- Network Monitoring and Protection

Amazon Web Services complies with **more than 50** global certifications, attestations, frameworks and regulations, making it certifiably the most secure cloud storage and compute platform available.

AWS has proven itself to be a strong cloud partner to many of today's biggest, fastest, and most innovative companies, and Mango leverages the power of AWS to deliver our powerful, secure online GIS platform that makes deploying web maps seriously simple.

Mango

Complete control to ensure your most precious asset is protected.

	Signed in Users				Not Signed in
	Account Owner	**Administrators**	**Data Editors**	**Private Viewers**	**“the public”**
MAP & DATA ACCESS					
View Public Maps	✓	✓	✓	✓	✓
View Standalone Maps	✓	✓	✓	✓	🔗
View Hidden Maps	✓	✓	✓	✓	🔗
View Password Protected Maps	✓	✓	✓	✓	🔒
View Internal Maps	✓	👥 or ✏	👥	👥	✖
View Offline Maps	✓	👥 or ✏	👥	👥	✖
View Public Datasets	✓	✓	✓	✓	✓
View Internal Datasets	✓	👥 or ✏	👥	👥	✖
MAP ACTIONS					
Add Public Datasets to maps	✓	✓	✖	✖	✖
Add Internal Datasets to maps	✓	👥 or ✏	✖	✖	✖
Create & Modify Maps	✓	👥 or ✏	✖	✖	✖
DATASET ACTIONS					
Upload Data	✓	✓	✖	✖	✖
Reupload Data	✓	👥 or ✏	👥	✖	✖
Edit Feature Attributes	✓	👥 or ✏	👥	✖	✖
Edit Geometry	✓	👥 or ✏	👥	✖	✖
ACCOUNT ACTIONS					
Create Users	✓	✖	✖	✖	✖
Edit Users	✓	✖	✖	✖	✖
Create Groups	✓	✖	✖	✖	✖
Edit Groups	✓	✖	✖	✖	✖
Modify Plan & Add-ons	✓	✖	✖	✖	✖
Modify Billing Information	✓	✖	✖	✖	✖

✓	Access
✖	No Access
✏	Only if user created the map or dataset
👥	Only if user belongs to a Group with appropriate permissions
🔗	Only with map’s unique URL
🔒	Only with map’s unique password

Still have questions?

If you still have questions about Mango, we'd love to talk!

You can request a demo from one of our amazing team members. Just click the link below to book an appointment, and we will be in touch!

Talk to you soon.

Book an appointment at www.mangomap.com/contact

Mango

The Simple Online GIS

Make Amazing Interactive Web Maps That You and Your Users Will Love!