aws partner network

Advanced
Technology
Partner

Businesses across the world need a cloud storage partner to provide a safe and secure way to discover and access their valuable data assets. Administrators also need a solution that can give them the full control and transparency they need to detect possible breaches and threats. With **Tictac DRaaS**, administrators can manage their data daily to ensure their mission critical data is being protected at all times.

This paper will detail the capabilities and backup policies available in **Tictac DRaaS**, to ensure administrators comply with data security regulations

Product Features

Admin Management

We understand that businesses operate differently. So, we've developed a number of capabilities to allow organizations to customize **Tictac DRaaS** in order to fit their individual needs, all from an easy-to-use console.

Add users

Tictac DRaaS provides 4 ways to add users:
Email invites: Simply type the email for the team members and they will receive instructions on how to join **Tictac DRaaS**.
Manual Add: Fill out the user's information, and then install the client software on their computer.

Active Directory Deployment: Deploy to all users via Active Directory Deployment. Ideal for large organizations.
Bulk Add via CSV: Add multiple users by uploading a CSV.

Data Selection

Administrators have the choice to either allow their users to select what data to back up, or they can remotely configure backup policies for their users. **Tictac DRaaS** also gives the option to filter file selection via file types, dates, or size.

Application Privileges

The Administrator has the ability to control the installed backup software on the user's machine. In addition, they can specify if the user can:
- Run Backups
- Pause/Resume Backups
- Exit the client
- Uninstall
- A pin can also be set to prevent unauthorized access to the app.

Web Access Privileges

Additionally, the administrator can granularly control user access to data with the following:

- Allow/deny sharing.
- Allow/deny the ability to delete data.
- Restrict password changes.
- Restrict users from changing the sign in email.
- Discovery privileges, which permits users to access data uploaded from the same group or from a centralized location.

Remote Restore

An admin can choose to access user data or remotely retrieve data to send to their teams. This can be done either by direct download, or by initiating a remote restore. It's important to note that the remote restore will push all data to the client's computer without any intervention.

User Account Management

As personnel come and go and old computers start to get replaced, it's imperative to have a user management system that is flexible and robust.

With our platform, administrators can manage user accounts by:
- Activating users
- Suspend users
- Deleting users
- Add computers
- Suspend computers
- Activating computers
- Archive computers
- Delete computers

Administrator Management

If your business needs more than one administrator, our platform can support that. The main admin of the account also has the flexibility to grant or restrict what capabilities the 2nd admin can or cannot use

Visibility

Tictac DRaaS provides complete transparency giving admins the ability to see activity reports on backup, bandwidth usage, system alerts, client locator and billing. A complete audit in Tictac DRaaS tracks the following:

- **User Management Tracking:** Create, suspend, activate and delete users.
- **User Access Tracking:** User login time, files accessed, search activity, download, video views, file shares, and file deleting.
- **Device Activity:** Device added to back up and restore activities, backup pausing/resuming, last backup date, storage alerts, device suspended, deleted or archived.

- **Administrator Activity:** Adding new policies, deleting policies, assigning policies and changing system settings, and adding new administrators.

Sharing security

Any file uploaded is protected by military-grade encryption, meaning your data is always safe. To give you greater peace of mind, we've added two extra security measures where you can password-protect shared files and set a time limit for any shared link.

Passwords for shared links

Any shared link can be protected with an owner-defined password. Before any file or folder data is transmitted, an access control layer verifies that the correct password has been submitted as well as meeting all other requirements (such as team, group, or folder ACL). Once this happens, a secure cookie is stored in the user's browser to remember that the password was verified previously.

Expirations for shared links

Users can set an expiration for any shared link to allow temporary access to files or folders.

Under the hood

Our mission is to create an innovative platform that is quick and easy-to-use. In order to achieve this, our team of in-house software engineers are always looking to evolve the architecture to improve speed data transfers, improve reliability for uploads, downloads and sharing.

In this section, we'll explain how data is transferred, stored, and processed securely.

Architecture

Tictac DRaaS is designed with multiple layers of protection, covering data transfer, encryption, network configuration, and application-level controls, all distributed across a scalable infrastructure. Users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to the platform. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices whenever files are added, changed, or deleted.

Our architecture is made up of the following services:

Encryption and application service

By design, **Tictac DRaaS** provides a unique security mechanism that goes beyond traditional encryption to protect user data. The Encryption and Application Services process files from **Tictac DRaaS** applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only the blocks that have been modified between revisions.

If the platform detects a new file or changes to an existing file, the application notifies the encryption and application services of the change, and new or modified file blocks are processed and transferred to the storage service.

Metadata service

Tictac DRaaS metadata is stored in a MySQL-backed database service, and is shared and replicated as needed to meet performance and high availability requirements. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and type. This helps support features like version history, recovery, and sync.

Protocol

The actual file block transfer is done over HTTPS. Each computer runs an HTTPS server with endpoints. A client will poll multiple peers to see if they have the blocks, but only download blocks from one server.

To keep all of your data safe, we make sure that only clients authenticated for a given folder can request file blocks. We also make sure that computers cannot pretend to be servers for folders that they do not control. To solve for this, we generate SSL key/certificate pairs for **Tictac DRaaS** or the shared folder. These are distributed from our servers to the user's computers and is then authenticated. The key/certificate pairs are rotated any time membership changes (i.e. when someone is removed from a shared folder). We require both ends of the HTTPS connection to authenticate with the same certificate (the certificate for **Tictac DRaaS** or the shared folder). This proves that both ends of the connection are authenticated.

When making a connection, we tell the server which file or folder we are trying to connect for by using Server Name Indication (SNI), so that the server knows which certificate to use.

Reliability

A storage system is only as good as it is reliable, and to that end, we've developed **Tictac DRaaS** with multiple layers of security to guard against data loss and ensure availability. **Tictac DRaaS** storage uses systems including third-party providers that are designed to provide 99.999999999% durability.

This feature, beyond protecting user data, provides high availability of the **Tictac DRaaS** service. In the event of a failed connection to the **Tictac DRaaS** service, a client will gracefully resume operation when a connection is re-established. Files will only be updated on the web if the file is completely and successfully validated with the **Tictac DRaaS** service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for the end user.

Business continuity

We maintain a business continuity plan (BCP) to address how to resume or continue providing services to users — as well as how to function as a company — if business-critical processes and activities are disrupted. Our BCP identifies internal and external threats and specifies how people, processes, and infrastructure will be mobilized to prevent and recover from disruptions.

Data centers

Tictac DRaaS corporate and production systems are housed at third-party subservice organization data centers and managed service providers located in the United States, Ireland, and Australia.

Subservice organization data center SOC reports are reviewed at a minimum annually for sufficient security controls. These third-party service providers are responsible for the physical, environmental, and operational security controls at the boundaries of **Tictac DRaaS** infrastructure. **Tictac DRaaS** is responsible for the logical, network, and application security of our infrastructure housed at third-party data centers.

Our current managed service provider for processing and storage is responsible for the logical and network security of **Tictac DRaaS** services provided through their infrastructure. Connections are protected through the managed service provider's firewall, which is configured in a default deny-all mode. **Tictac DRaaS** restricts access to the environment to a limited number of IP addresses and employees.

Encryption

Data in transit

To protect data in transit between our apps and servers, **Tictac DRaaS** uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 256-bit Advanced Encryption Standard (AES) encryption. File data in transit between a **Tictac DRaaS** client and the hosted service is always encrypted via SSL/TLS. For end points we use strong ciphers and support perfect forward secrecy and certificate pinning. Additionally, on the web we flag all authentication cookies as secure and enable HTTP Strict Transport Security (HSTS) with subdomains enabled.

To prevent man-in-the-middle attacks, authentication of **Tictac DRaaS** front-end servers is performed through public certificates held by the client. An encrypted connection is negotiated before the transfer of any files and ensures secure delivery of files to **Tictac DRaaS** front-end servers.

Data at rest

Tictac DRaaS files at rest are encrypted using 256-bit Advanced Encryption Standard (AES). Files are primarily stored in multiple data centers.

Network security

Tictac DRaaS diligently maintains the security of our platform network. Our network security and monitoring techniques are designed to provide multiple layers of protection and defense. We employ industry-standard protection techniques, including firewalls, network vulnerability scanning, network security monitoring, and intrusion detection systems to ensure only eligible and non-malicious traffic is able to reach our infrastructure.

Our internal private network is segmented according to use and risk level. The primary networks are:

- Internet-facing DMZ
- VPN front-end DMZ

■Production network
■Corporate network

Access to the production environment is restricted to only authorized IP addresses and requires multi-factor authentication on all endpoints. IP addresses with access are associated with the corporate network or approved **Tictac DRaaS** personnel. Authorized IP addresses are reviewed on a quarterly basis to ensure a secure production environment. Access to modify the IP address list is restricted to authorized individuals.

Traffic from the internet destined to our production network is protected using multiple layers of firewalls and proxies.

Strict limitation is maintained between the internal **Tictac DRaaS** network and the public internet. All internet-bound traffic to and from the production network is carefully controlled through a dedicated proxy service and those, in turn, are protected by restrictive firewall rules.

Tictac DRaaS uses a sophisticated tool to monitor laptops, desktops and production systems for malicious events. All security logs are collected in a centralized location for forensic and incident response, in line with industry standard retention policy.

Physical security

Infrastructure

Physical access to subservice organization facilities where production systems reside are restricted to personnel authorized by **Tictac DRaaS**. Any individuals requiring additional access to production environment facilities are granted that access through explicit approval by the administrator.

A record of an access request and approval is always recorded in **Tictac DRaaS**. Once approval is received, a responsible member of the infrastructure team will contact the appropriate subservice organization to request access for the approved individual. The subservice organization enters the user's information into their own system and grants the approved **Tictac DRaaS** personnel badge access and, if possible, biometric scan access. Once access is granted to approved individuals, it is the data center's responsibility to ensure that access is restricted to only those authorized individuals.

Compliance

Tictac DRaaS is a Payment Card Industry Data Security Standard (PCI DSS) compliant merchant. However, **Tictac DRaaS** Business is not meant to process or store credit card transactions. **Tictac DRaaS** provides customers with a PCI Attestation of Compliance (AoC) for our merchant status.

HIPAA/HITECH. **Tictac DRaaS** signs Business Associate Agreements (BAAs) with customers who require them in order to comply with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HI-TECH).

Tictac DRaaS makes available a mapping of our internal practices and recommendations for customers who are looking to meet the HIPAA/HITECH Security and Privacy Rule requirements with **Tictac DRaaS** Business.

Customers interested in requesting these documents or signing a Business Associate Agreement with **Tictac DRaaS** Business can reach out to their account manager or contact our sales team.

Privacy

People and organizations trust **Tictac DRaaS** with their most important work files every day, and it's our responsibility to protect those files and keep them private.

The **Tictac DRaaS** Privacy Policy, Terms of Service, and Acceptable Use **Policy** provide notice of the following terms:

■ What kind of data we collect and why.
■ With whom we may share information.
■ How we protect this data and how long we retain it.
■ Where we keep and transmit your data.
■ What happens if the policy changes or if you have questions.

Summary

Tictac DRaaS offers easy-to-use tools to discover data like a private search engine, while providing the security measures and compliance certifications all organizations require. With a multi-layered approach that combines a robust infrastructure with a set of customizable policies, **Tictac DRaaS** is placing the control of data back into your hands. If you'd like to learn more about how **Tictac DRaaS** can help your business, email our sales team at
info@tictac.gr

About **Tictac DRaaS**

The amount of unstructured data is a growing problem for businesses. We solve this with **Tictac DRaaS**. The technology allows you to discover your big data just like a search engine – quick and secure. Our innovative platform is made with you in mind. The user experience is focused on simplicity. But that's not all, in just a few clicks, you secure all your critical data with military-grade encryption.

That's why more than 3 million users across the world count on **Tictac DRaaS**.

Tictac Data Recovery & Cyber Security
Tichis 2, Elliniko, Greece