Security and resilience provisions

TEXECOM DIGITAL SERVICES

- **TEXECOM CLOUD** -The tools to manage, configure and control your alarm system and Texecom Connect app portfolio.
- **TEXECOM MONITOR** - Primary alarm signaling to Alarm Receiving Centres.
- **TEXECOM CONNECT** - Mobile application enabling users to control their alarm systems.

DATA COMPLIANCE

Texecom Digital Services, incorporating Texecom Cloud Services (TCS), is designed and operated using industry standard best practices with partners who can be trusted. The solution meets the requirements for Cyber security outlined by Cyspag.

DATA PRIVACY

The services are designed to comply with data privacy requirements in the UK, Europe (GDPR) and how we handle Installer and End user data is outlined in our data privacy policy.

SERVER LOCATIONS

Texecom Digital Services are hosted on Amazon Web Services (AWS) deployed in the AWS Ireland hub.

DIGITAL SECURITY MEASURES

Security is critical to the provision of Cloud Services for alarm systems and Texecom take that responsibility seriously. TCS is designed to be a completely secure digital environment and security implications are considered for every change and enhancement of the service and then validated by our internal test teams before deployment.

PHYSICAL SECURITY

Texecom use AWS because their services are trusted by a huge range of online service providers. AWS solutions are contained within secure premises that Amazon ensures are only accessible to approved people and the data layer is only accessible to us the clients. Details can be found here :

https://aws.amazon.com/compliance/data-center/data-centers/

INTERNAL ADMINISTRATION

Within Texecom we have a strict security policy governing the provisions of system administration access. This is split into specific roles and access is only available to the tasks that those individuals require. Super user access (System Admin) is only provided to those that require access, which is limited to a small number of devops staff who maintain the system. This is only provided once signed off by a Director of the organisation.

All Texecom employees who manage customer accounts on the Texecom digital services are trained fully on security procedures for managing customer data and are only provided access to systems once they have signed that they understand the security implications of their work. All employees in that position also have to use multi factor authentication to log in to services.

ALARM TRANSMISSION EN50136-2 COMPLIANT

LOSS PREVENTION CERTIFICATION BOARD LPCB 717q SmartCom 4G/SmartCom

Security and resilience provisions

USER ACCOUNT AUTHENTICATION

All access to TCS is via the web service API, this is secured using Usernames and Passwords. We require passwords that contain at least 8 characters and enforce the requirement for letters and numbers. This uses 0Auth authentication in common with most web based secure solutions. We encourage customers to request employees to set their own passwords and suggest that they change them regularly. Installer account requests require a valid email as their username to receive notification or password resets. We offer the facility for customers to use Multi Factor Authentication so that they can enforce this for their employees.

DATA SECURITY

Data is secured at rest on the Cloud service. The database is encrypted and therefore is only accessible via the API to all users including Texecom. This prevents hacked data theft at source. Access to data tables is available to Texecom System Administrators to enable us to manage systems and to provide anonymized reporting. We provide the option to Installers to access and encrypt the service data using an additional password. This prevents the site information data (including address details and contact details) from being accessed by anyone without authorisation.

Credit card and bank information is not held on Texecom Servers. Texecom use Barclaycard and GoCardless to provide secure card and bank payment services, where all client-server communication is 256-bit SSL encrypted. Texecom hold a validated secure token for each card or customer to enable payment processing. These tokens are only valid when used from our defined servers by IP address and our authenticated company account.

DEVICE SECURITY

Texecom services are connected using the Texecom SmartCom and SmartCom 4G Communicators. These communicators are designed to connect only to the URL end points that we define.

https://cloud.texe.com

https://broker.texe.com

Both of these are over port 443 as outgoing connections only. There is no requirement to open incoming ports for the operation of Texecom Digital Services.

Outgoing event communication from the SmartCom to the Texecom Cloud is direct to cloud.texe.com.Where communication of data is required to be sent to the SmartCom or Security panel, this is done via the MQTT broker for IP communication. Where mobile networks are used, this is a direct fixed NAT IP communication.

SmartCom's negotiate their connection and user credentials on first connection. They generate their own username and password based on a unique identifier. Once these have been passed on registration to the cloud, all other communication is authenticated using these credentials.

Communication over the mobile networks is via our own APN and private data SIM provision.

SERVICE AND PRODUCT MANAGEMENT

Texecom communicates service and product software updates by email directly to Installer customers prior or at the time of the update. In the event that support for a service or product is to be withdrawn for whatever reason, Texecom will communicate to installers the change in status and actions that the installer should take. This will be sent out to all registered digital service installer users, distributors and partners.

VULNERABILITY REPORTING

If customers identify a service vulnerability, then this should be reported by email to cloud@texe.com. Texecom will acknowledge and immediately investigate and respond in full. If a vulnerability is found, Texecom will resolve in a timely manner and will communicate to specific users if this has resulted in security or data compromise.

Texecom monitor | Security and resilience provisions

LINK SECURITY

All communication from the users interface via the web API is over https secured using TLS1.2.

This is a certificated service using public certification of each authenticated session.

All communication from the SmartCom to the Cloud service utilises MQTTS which uses TLS1.2 as well.

MQTT services are used with closed end points, only devices and software provided by Texecom can authenticate with the MQTT brokers.

The communication uses SHA-2 256 bit encryption for all communications, ensuring that it is virtually impossible, even with substantive technology to be able to break into and read or direct changes to an alarm panel or the Cloud service.

RESILIENCE

The Texecom Cloud Service is a resilient platform. It is based on secure technologies. Throughout the service we have built in redundancy at every level, to ensure that we can support the scalability of the service. There are duplicate DNS services for each of the servers that direct to each of the brokers and servers. Each end point operates via load balancers to multi-redundant servers (a minimum of 5 currently). If there is a peak in demand, the service will automatically scale and run up additional servers in the pool. This occurs transparently to any users. We use a federated MQTT broker which ensures that there is machine and service redundancy for the broker service.

Our connections to ARC's are all replicated paths and replicated end points. These are monitored normally with a poll rate of 30 seconds. We often know of problems at an ARC before the ARC is aware of them.

SERVICE MONITORING

All our services are monitored using the Zabix Service Health Platform which monitors over 1000 system metrics and communicates the required actions until issues are resolved using Pager duty. This includes escalation to on call Engineers, management and Directors, 24 hours a day, 7 days a week, 52 weeks of the year.

Our current up time for Texecom Cloud and Texecom Connect service over the last 18 months is 100%.

SECURITY AUDITS

Texecom complete internal security audits on a quarterly basis. Actions are reviewed and completed within the next quarter. If a severe risk were to be uncovered then this would be dealt with immediately.

Texecom complete external audits of our service design and implementation on an ad hoc basis when we have made major changes, or at least every 3 years. In 2023 external audits will increase to an annual audit.

DATA PRIVACY

Texecom have a full data privacy policy for all our services. These can be found following these links:

Texecom Cloud: https://cloud.texe.com/public/publicdocs/download?publicdoc_ref=privacy

Texecom Connect: https://cloud.texe.com/public/publicdocs/download?publicdoc_ref=privacyapp

TEXECOM TERMS AND CONDITIONS

Texecom Cloud: https://cloud.texe.com/public/publicdocs/download?publicdoc_ref=NewTerms

Texecom Connect: https://cloud.texe.com/public/publicdocs/download?publicdoc_ref=termsapp

SECURE & SUPPORTED

Texecom Monitor is one of the most advanced secure alarm communications providers available. Featuring state-of-the-art cyber security, multi-path and multi-redundancy resiliency, providing a scalable, expandable, and always available service via cloud system architecture. Texecom Cloud Service and Texecom Monitor is an alarm signalling and cloud management solution you can depend on.

ALARM TRANSMISSION EN50136-2 COMPLIANT

LPCB LOSS PREVENTION CERTIFICATION BOARD 717q SmartCom 4G/SmartCom