

White Paper

Cloud Services for Secure Alarm Handling

This is Skyresponse:system

Skyresponse:system – the unique alarm and event handling system from Skyresponse – forwards alarms from digital, Internet connected products to respondents/response centres using a decentralized, cloud based, IT platform. The system ensures that all connected units will forward their alarms and the related information, following flexible rules, to the most appropriate receiver at any time.

Skyresponse:system includes a web based administrative system (*Skyresponse:admin*) for the services offered, the *Skyresponse:central* web-based response centre, the *Skyresponse:mobile* alarm reception apps, the *Skyresponse:alarm* apps for generation of alarms, and various accessories.

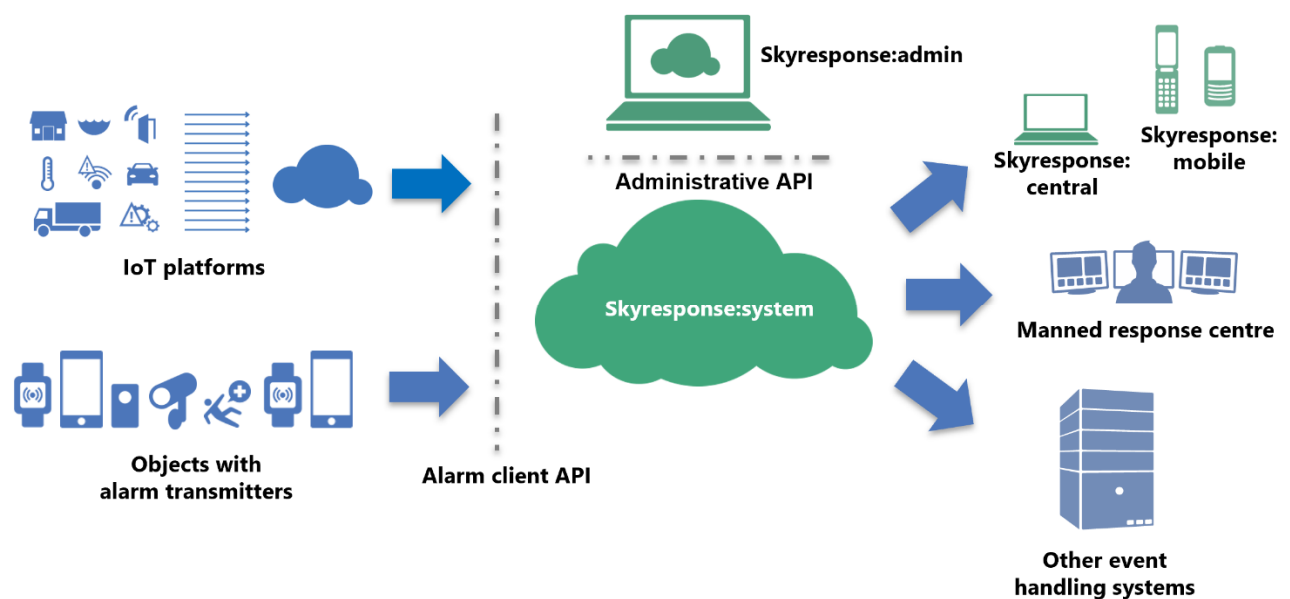


Figure 1. *Skyresponse:system* – a complete, cloud based, alarm and event handling system

From the beginning on Skyresponse:system has been designed to leverage two major trends in IT systems design: Ubiquitous connectivity over the Internet and cloud computing using a multitenant architecture. With the central logic of the platform implemented as a cloud service reachable over fixed and mobile broadband, the alarm service becomes independent of any specific computer hardware. Execution of the logic is shared between several, geographically separated, clusters of servers, and wherever the user

has Internet connectivity, he/she can both raise an alarm and act as a respondent to alarms.

Furthermore, Skyresponse:system is using a multitenant software architecture within the cloud. In a multitenancy environment, multiple tenants (customers) share the same application, running on the same operating system, on the same hardware, with the same data-storage mechanism. The distinction between the customers is instead achieved during application design, thus customers do not in any way share or see each other's data. With this architecture all software development can be concentrated towards one single code base and the release process and quality control of applications become more efficient when compared to using a traditional architecture with dedicated software packages per tenant.

The Cloud

Cloud computing has gained widespread use over the last few years. With the exponential increase in data use, it is becoming more and more difficult for individuals and organizations to keep all their vital information, programs, and systems up and running on in-house computer servers.

By hosting applications and databases remotely, the cloud servers free up memory and computing of individual, local computers. Users can instead securely access cloud services using credentials received from the cloud service provider.

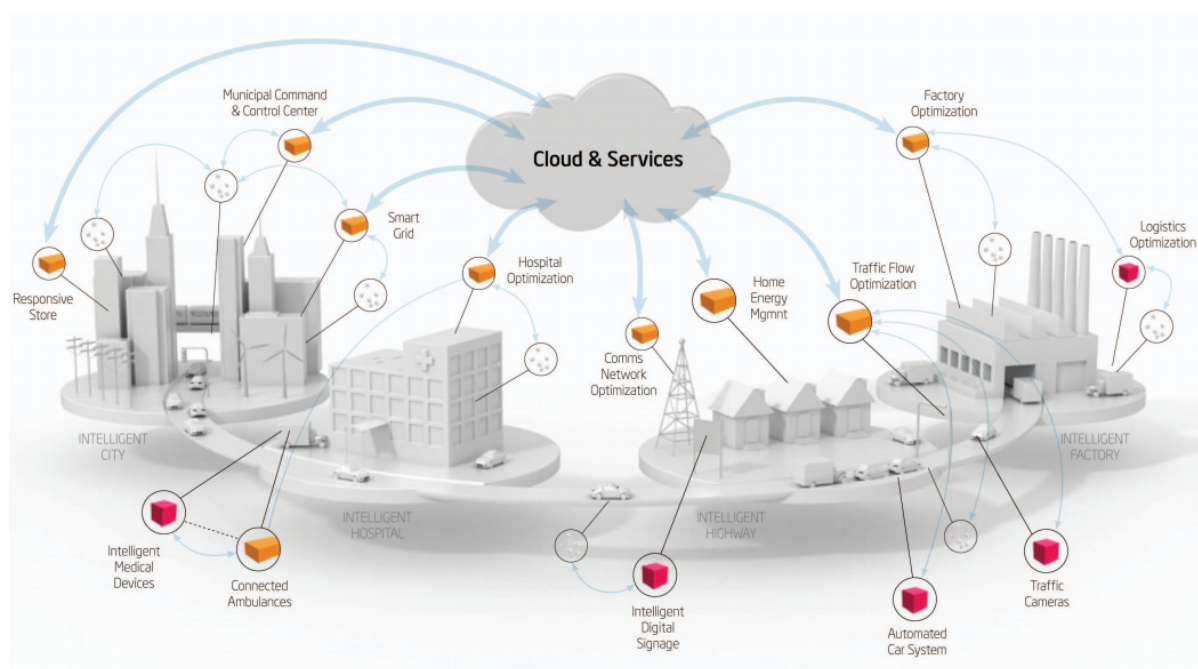


Figure 2. The Cloud

Cloud services can be hosted at and made available by many types of data centres. For essential services, such as event and alarm handling, confidentiality, integrity and availability characteristics of the selected platform plays a prominent role. For legal reasons, storage and handling of sensitive data may put additional requirements on the geographical location of the data centre providing the service. After a long and careful evaluation

of these aspects Skyresponse AB has selected the market leading *Amazon Web Services (AWS)* as the basis for implementing Skyresponse:system.

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offering over 165 fully featured services from data centres globally. Millions of customers — including the fastest-growing start-ups, largest enterprises, and leading government agencies — trust AWS to power their infrastructure, become more agile, and lower costs.

Companies around the world are moving to a cloud-based infrastructure to increase IT agility, gain unlimited scalability, improve reliability, and lower costs. They want the flexibility to expand their operations at a rapid pace without worrying about setting up new IT infrastructure. They want to enhance their end-user and customer experiences by minimizing latency, the time it takes for their data packets to travel, so they can avoid delays and interruptions. As well, customers want to be able to easily support any country-specific data sovereignty requirements, which means they need the flexibility to have a wide selection of geographic regions of data centres from which to choose to deploy their application workloads.

The AWS Global Infrastructure delivers a cloud infrastructure companies can depend on — no matter their size, changing needs, or challenges. The AWS Global Infrastructure is designed and built to deliver the most flexible, reliable, scalable, and secure cloud computing environment with the highest quality global network performance available today. Every component of the AWS infrastructure is designed and built for redundancy and reliability, from regions to networking links to load balancers to routers and firmware.

The AWS Cloud has a global reach with local datacentres on multiple continents.

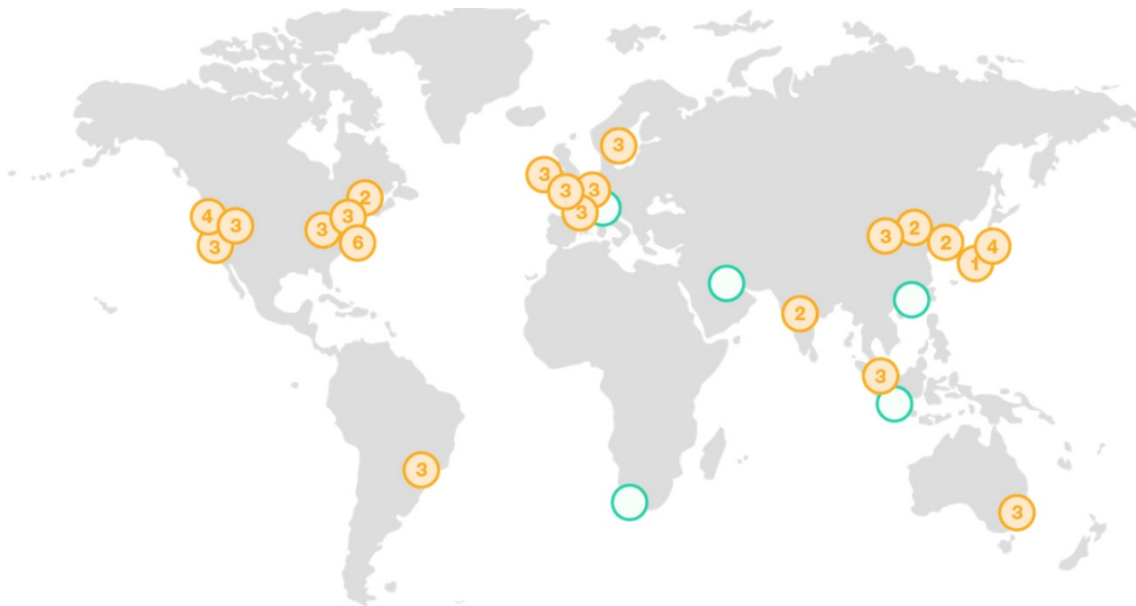


Figure 3. Existing (yellow) and planned (green) Amazon Web Services' availability zones within geographic regions around the world as of April 2019.

The Key Benefits of Cloud Services

Traditionally, alarm handling systems have been based on sensors and alarm transmitters sending alarms over analogue or digital networks to hardware located directly at the alarm response centre (ARC). The local hardware also provides local storage of relevant user and object information, and response centre operators are presented the alarms on displays directly connected to the on-site response centre computing hardware.

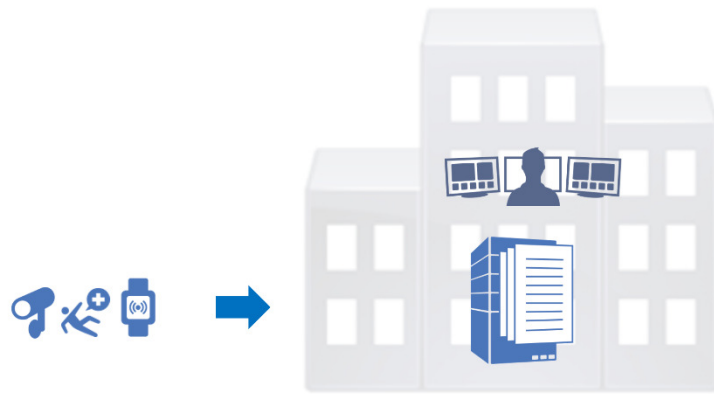


Figure 4. A response centre using a traditional, on-site and local IT system.

Implementing an alarm handling service such as Skyresponse:system as a cloud-based application addresses an old problem with new technology. What benefits does it bring and what problems may occur?

Availability

A key advantage of a cloud service for alarm handling is its superior availability compared to all types of local solutions. The business idea of the cloud service provider is to sell compute capacity. He therefore has made substantial investments in ensuring that the services he offers are always up. These investments include physical and geographical redundancy at all levels, software tools to make maximum use of the infrastructure, 24/7 availability of technical staff, secure location of hardware and much more. AWS has for example access to experts in every relevant field, such as storage, firewalls, security and communications, which translates into a minimal risk for human errors when configuring the involved hardware and software. Establishing the same level of operational availability of a computing platform is just not possible for a local, single purpose, installation, considering the associated costs.

Cloud infrastructure can also help you with data loss prevention and disaster recovery. If you rely on a traditional on-premises approach, all your data will be stored locally. Despite your best efforts, computers can malfunction from various reasons, from malware and viruses, to age-related hardware deterioration and simple user error.

But, when uploaded to the cloud, the data and the code creating the alarm handling service can be duplicated and replicated as required, while remaining accessible from any computer with an Internet connection and the right permissions. There is no need for cumbersome back-up routines locally, all back-up and replication are automatically performed by the cloud service provider.

You may argue that a cloud service becomes more dependent on the involved communication network providing the Internet connections. However, given the current availability of the fixed and mobile networks and the routing capabilities of the Internet, the possible down time of any communication links does not contribute measurably to the general un-availability of the entire alarm handling service. In addition, the connections with a cloud-based response centre has in general a much higher level of redundancy and better availability than what can be afforded for a local IT system.

Building on the multi-site and redundancy capabilities of AWS, Skyresponse:system operates on and meets targets of availability above 99,995% for the alarm distribution services. Service recovery is virtually instantaneous and without any loss of data, thanks to the auto healing inherent when using AWS.

Confidentiality and Integrity

A major concern that many organizations have when it comes to adopting a cloud computing solution is the issue of confidentiality and integrity. After all, when files, programs, and other data are not kept securely on your site, how can you know that they are being protected? If you can have remote access to your data, then what's stopping some cybercriminal from doing the same thing? Well, quite a bit, actually.

For one thing, a cloud service provider's full-time job is to carefully monitor security, which is significantly more efficient than a conventional in-house system, where an IT organization must divide its efforts between a myriad of IT concerns, with security being only one of them. And while most businesses do not like to openly consider the possibility of internal data theft, the truth is that a staggeringly high percentage of data thefts occur internally and are perpetrated by employees. When this is the case, it can actually be much safer to keep sensitive information off-site.

Confidentiality and regulations compliance is a shared responsibility between AWS and Skyresponse. AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Skyresponse assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud.

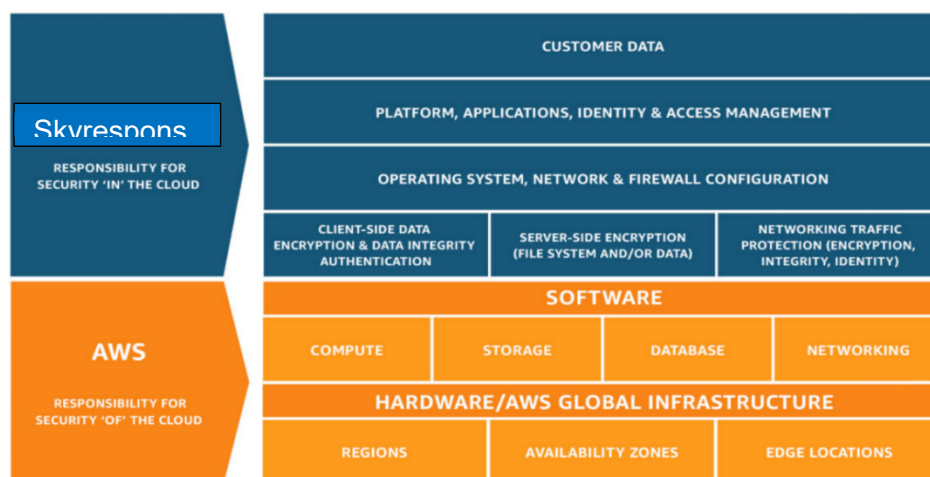


Figure 5. Responsibility for security is divided between Skyresponse and AWS

A major factor contributing to the improved security is the encryption of all data being transmitted over networks and stored in databases. By using encryption, information is less accessible by hackers or anyone not authorized to view your data. As an added security measure, different security settings and permissions can be set based on the user logging in to the service.

Flexibility and Scalability

Cloud based solutions are ideal for businesses with growing or fluctuating capacity demands. Thanks to the scalability of the AWS platform, it has for example been possible for Skyresponse to grow the number of handled alarms by more than 2000 times in less than three years. The number of handled and distributed alarms varies over the course of the day and thanks to AWS autoscaling capabilities the computational capacity automatically scales up and down with the number of alarms. In addition, the cloud-based response centre is ideally suited to handle transient high load situations, e.g. when alarms are flooding in at a major event. This level of agility can give an organization using cloud-based alarm handling a real advantage over competitors. The flexibility can also be used to more easily test and verify new functions in the cloud than if you were to create test environments in a local system.

A cloud service offers more flexibility overall versus hosting on a local server. And, if you need extra capacity, the cloud-based service can meet that demand instantly, rather than undergoing a complex and expensive update to your IT infrastructure. This improved freedom and flexibility can make a significant difference to the overall efficiency of your organization.

This scalability also minimizes the risks associated with in-house operational issues and maintenance. You have high-performance resources at your disposal with professional solutions and zero up-front investment. Flexibility and scalability are key advantages of using a cloud-based alarm handling service.

Mobility and Ubiquitous Access

With an alarm handling service implemented as a cloud service, alarms can be generated anywhere where there is Internet access. This means that you can easily scale your response centre to cover whatever geographical region you are interested in. But even more important is that you can also distribute the entire response centre and the reception and handling of alarms at your will. A respondent to alarms only needs a computer with a web browser or a Smartphone with the Skyresponse:mobile app plus the correct log-in authorization, to receive and act upon alarms and notifications.

This full mobility of respondents when handling alarms opens for completely new operational processes and workflows in applications such as digitalized elderly care, facility management and dispatch of service personnel. Alarms and notifications can now be pushed directly to the respondent's Smartphone, where he/she can retrieve all information necessary to fulfil the task.

All alarm related information in the cloud can be easily retrieved, recovered, and processed with just a couple of clicks. Respondents can get access to alarms and event information on-the-go, 24/7, via any devices of their choice, in any corner of the world as long as they are connected to the Internet. Considering the more than 2.6 billion Smartphones used worldwide, this means that you can create truly mobile alarm and event handling offerings when using a cloud-based alarm handling service.

Competitiveness and Automatic Updates

A cloud service provider such as AWS runs applications for myriads of customers, giving a significant economy of scale in computing. The economy of scale enables the cloud service provider to stay on top of the technical development, always using the most up to date technology, the best performing servers, and the most efficient supporting software for the customers' applications. In contrast, a local system is dependent on local IT support with limited resources and technical competence when compared to the resources of the cloud service provider.

On top of that, all the upgrades and updates of the hardware and operating software for the alarm handling service are done automatically, by AWS. This saves time and team effort in maintaining the systems, tremendously reducing the IT team workloads and reduces the risk of using outdated software. In addition, using the redundancy features of AWS it becomes possible to keep the service "always on", also during maintenance and updates with new releases, a major advantage in mission critical applications such as alarm handling.

Cost Savings

From the advantages listed above, it is obvious that implementing a cloud-based alarm handling service also leads to significant cost savings. Work processes can be made more efficient, for example by distributing alarms directly to field staff, IT-systems cost can be reduced, and less expensive IT systems expertise is needed within your organization. Furthermore, the cloud-based system can be tailored to your precise needs and with pay-as-you-grow model you will only pay for the capacity you are actually using.

When using a cloud-based service, you do not have to spend huge amounts of money on purchasing and maintaining equipment. This drastically reduces CAPEX costs. You do not have to invest in hardware, facilities, utilities, or building out a large data centre to grow your business. You do not even need large IT teams to handle your response centre operations, as you can enjoy the expertise of your cloud provider's staff.

A cloud-based service also reduces costs related to downtime, given that the correct agreements and SLA standards have been set. Since downtime is rare in cloud systems, this means you do not have to spend time and money on fixing potential issues related to downtime.

Infrastructure Availability and Security

Infrastructure Availability

The AWS Global Infrastructure is designed and built for redundancy and reliability, from Regions to networking links to load balancers to routers to firmware. For example, in order to offer maximum resiliency against system disruptions, AWS builds its data centres in multiple geographic Regions as well as across multiple Availability Zones (AZs) within each Region. Each Region is isolated from the others. And AWS Availability Zones are implemented in completely separate buildings kilometres apart for complete redundancy.

Infrastructure Security

As described above, responsibility for Skyresponse:system security is a shared undertaking by AWS and Skyresponse: Skyresponse:system is built as an alarm handling service on top of the Amazon Web Services (AWS). It therefore relies upon the advanced security features of AWS for its fundamental security.

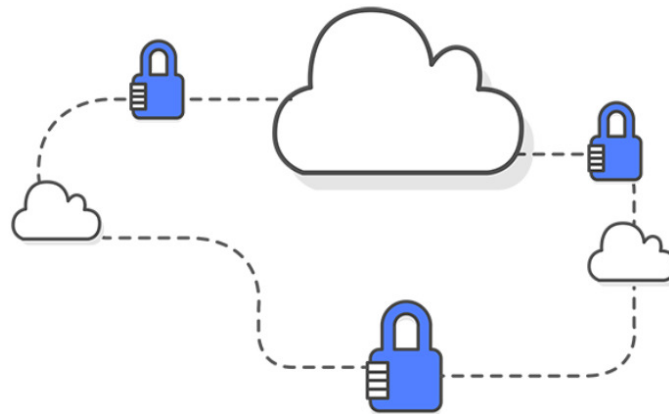


Figure 6. Skyresponse:system leverages the AWS infrastructure and security architecture.

Security at AWS starts with the core infrastructure. Custom-built for the cloud and designed to meet the more stringent security requirements in the world, the AWS infrastructure is monitored 24/7 to help ensure the confidentiality, integrity, and availability of AWS customers' data. Customers can build on the most secure global infrastructure, knowing they always own their data, including the ability to encrypt it, move it, and manage retention.

Skyresponse:system Security

Role Based Data Access

Skyresponse:system employs a role based user access model, which ensures that anyone logging in to the system only will get access to exactly the data that is needed for the role. A sophisticated classification scheme for alarms and events ensures that the alarm

only is distributed to the correct receiver. Furthermore, the alarm presentation can also be adapted to only show required information to the operator receiving an alarm.

Authentication of Users

All administrators and respondents of Skyresponse:system are authenticated at log in. For persons having a role with more extensive authorities, such as a system administrator, two-factor authentication is required for higher level security. In addition, all actions by administrators and respondents are logged and can be analysed off-line.

Encryption of Stored Data

All data used by Skyresponse:system is stored in encrypted format by AWS. The encryption keys are available to Skyresponse and no one else. Data is also encrypted when being sent to/from a web interface and the Skyresponse apps for mobile phones. If an alarm transmitter supports encrypted transmission of alarm data, this data will be encrypted when an alarm is raised.

Data encryption capabilities available in AWS storage and database services include:

- Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS.
- Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, satisfying advanced compliance requirements.

Logging

Skyresponse:system logs all events taking place in the system, including who is logged in, who takes an alarm and what actions that are taken by respondents and administrators. The logs can be analysed off-line to evaluate how the system and its users have acted on the information they have had access to.

Penetration Tests

To ensure system security, Skyresponse regularly performs penetration tests, i.e. authorized simulated cyberattacks performed to evaluate the security of Skyresponse:system. The tests are performed to identify both weaknesses including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

ISO Certification

Skyresponse holds both ISO 9001 and ISO27000 certifications. While ISO 9001 focus on the quality management system ISO 27000 focus on Information Security Management System within Skyresponse and Skyresponse system. Even though it is possible to get certifications without using cloud systems, AWS well documented and shared responsibility model made Skyresponse ISO certification easier and more robust.

Legal Aspects

GDPR

Skyresponse:system has been prepared for GDPR (General Data Protection Regulation) compliance since the introduction within the European Union in May 2018. Skyresponse:system builds on a modern cloud based architecture where the customers can feel secure that their data is handled according to the regulation. Skyresponse:system is used as a multitenant solution where our Value Added Resellers uses branded versions to sell our products to both public and private sectors of the market. By signing Data Processing Agreements as a Processor with our customers and as a Controller with our suppliers such as Amazon, we maintain transparent information on how and where the data is processed.

Summary

Skyresponse:system is a cloud based and future proof platform for flexible and secure handling of alarms and other events in an emerging Internet of Things world. Thanks to the great flexibility of the platform, it is well suited for IoT applications in many different areas such as personal safety, personal care, and in the smart city.

From the beginning on Skyresponse:system has been designed to leverage the advantage of being a cloud service. This gives the system a unique level of availability, integrity and flexibility, while reducing both CAPEX and OPEX for the Skyresponse customers. Relying upon the advanced security features of Amazon Web Services and combined with the Skyresponse ISO 27000 certified design and operations practices, all user data resides safely within the system.



Skyresponse AB
Eriksbergsgatan 10B, 3tr
S-114 30 Stockholm, Sweden

skyresponse.com

sales@skyresponse.com | +46 8 409 115 70