

Security Incident Policy

Qualsys Ltd



Our software reduces compliance burden associated with regulations and standards:



An effective management system takes more than a single software solution or achieving a certificate for the wall. It takes time, energy, commitment and investment.

Qualsys's software and solutions give businesses the tools and knowledge they need to effectively plan, monitor and improve performance.

We've worked with worldwide brands such as Sodexo, BT and Diageo, as well as hundreds of SMEs, to help them make good practice natural and invisible.

Founded in 1995, Qualsys Ltd is now one of the largest privately-owned governance, risk and compliance software providers in the UK.

Our software solutions are used every day in more than 100 countries across the globe, helping all kinds of businesses meet a wide range of standards and regulations.



www.qualsys.co.uk

Get in touch

Chris Webster
Operations and Infrastructure
Manager
+44(0) 114 282 3338
Chris.Webster@qualsys.co.uk

Brands we work with



Welcome to our security incident policy



Chris Webster

Operations and
Infrastructure Manager,
Qualsys

Chris.Webster@qualsys.co.uk

Data and information security breaches are increasingly common occurrences, whether these are caused through human error or via malicious intent.

As technology trends change and the creation of data and information grows, there are more ways data can be breached.

Qualsys has a robust and systematic process for responding to any reported data or information security breach. This will ensure that Qualsys can act responsibly and protect our information assets as far as possible.

The goal of this document is to provide you with an overview of our security incident policy.

Our security incident policy

With regards to personal data, Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

For data processing to be lawful under GDPR, it is important that the lawful basis is established. Please see below for guidance on data processing:

- Consent of the data subject is sought as required
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- . Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

There are many rights that individuals hold with regards to their data. GDPR provides the following rights for individual:

- The right to be informed
- The right of access
- .The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

A Security Incident can be defined as a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

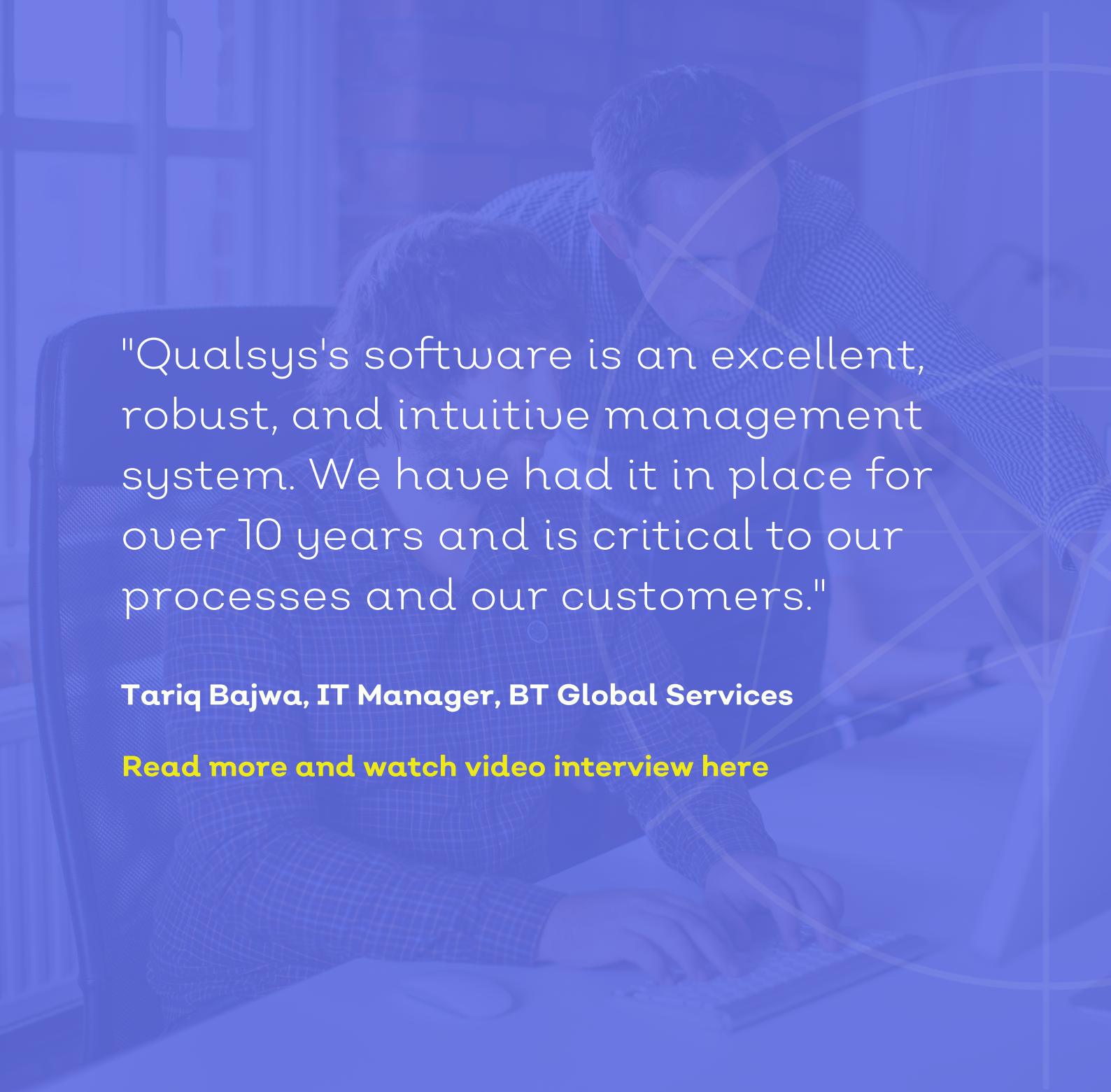
A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

All events should be managed in the same way and this is detailed below. Information security incidents should be reported through the appropriate channels, as described below, as quickly as possible.

On detection of any potential threat or event, the Quality Manager (and Data Protection Officer) is notified immediately. If not available, then the Operations and Infrastructure Manager or Technical Director should be notified and if they aren't available then another member of the Management team.

The following are examples of situations that need to be reported:

- Ineffective security controls
- Breach of data or information integrity, confidentiality or availability expectations
- Human errors
- Non-compliance with policies and procedures
- Breaches of physical security incidents
- Uncontrolled system changes
- Malfunctions of hardware or software
- Access violations



"Qualsys's software is an excellent, robust, and intuitive management system. We have had it in place for over 10 years and is critical to our processes and our customers."

Tariq Bajwa, IT Manager, BT Global Services

[Read more and watch video interview here](#)

Contact details

Aizlewood's Mill, Nursery
Street, Sheffield, S3 8GG

info@qualsys.co.uk
+44 (0) 114 282 3338
www.qualsys.co.uk

Talk to us

Questions about our security incident management policy? Talk to a domain expert today by calling or emailing us.

