Data Breach Policy

1.0 Policy statement

A data security breach is considered to be any loss of, or unauthorised access to, British Toxicology Society (BTS) data. Data security breaches include the loss or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorised use, human error (e.g. information sent to the incorrect recipient), hacking attacks and 'blagging' where information is obtained by deception.

2.0 Policy scope

This policy is relevant to all BTS members and data processors.

3.0 Definitions

Data breach - data that should be confidential is accessed or potentially could have been accessed by individuals without permission.

4.0 Procedures

Data security breaches will vary in impact and risk depending on the content and quantity of data involved, the circumstances of the loss and the speed of response to the incident. Breaches can result in significant fines and reputational damage. They may require substantial time and resources to rectify the breach.

The following procedure outlines the main steps in managing a breach and will help ensure that all breaches are dealt with effectively and efficiently. This procedure outlines the four stages (4.2 to 4.6 below) which should be completed following the initial containment of the breach. The individual stages may run concurrently.

4.1 Record keeping

Throughout the breach management process, records should be kept of what action has been taken and by whom. Appendix C provides an activity log template to record this information, in addition copies of any correspondence relating to the breach should be retained.

4.2 Security breach procedure

4.2.1 Containment & recovery

As soon as a data security breach has been detected or is suspected the following steps should be taken:

- Inform the Data Protection Officer and BTS President
- Identify and implement any steps required to contain the breach
- Identify and implement any steps required to recover any losses and limit the damage of the breach
- If appropriate inform the police

4.2.2 Assessment of risk

All data security breaches must be managed according to their risk. Following the immediate containment of the breach, the risks associated with the breach should be assessed in order to identify an appropriate response. The checklist in Appendix A should be used to help identify the exact nature of the breach and the potential severity, this information can then be used to establish the action required.

4.2.3 Notification of breach

You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. Also, if unaddressed, the breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Breaches should be assessed on a case-by-case basis. For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a committee telephone list, for example, would not normally meet this threshold.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.

A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

Breach notifications must contain:

- The nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned.
- The name and contact details of the data protection officer or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of BTS becoming aware of it. GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows for the information to be provided in phases.

If the breach is sufficiently serious to warrant notification to the public, BTS must do so without undue

Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2% of your global turnover.

The checklist in Appendix B: Notification of breach checklist, should be used to identify potential stakeholders who should be notified and to establish what information should be disclosed.

4.2.4 Evaluation and response

It is important to investigate the causes of the breach and evaluate BTS' response to the breach. A brief report on the breach, how it was dealt with and recommendations on how to prevent the breach reoccurring and similar risks should be written. Finally, if there are recommended changes to this procedure, such as additional information that would have been helpful or further explanation required, please contact your data protection officer.

5.0 Documents

Appendix A - Security breach risk assessment checklist
Appendix B - Notification of breach checklist.
Appendix C - Data breach activity log.

6.0 Related information:

BTS Privacy Policy
Information Commissioners Office
ICO guidance on data security breach management

Date of Review	February 2022
Date of Next Review	February 2024
Contact for document:	secretariat@thebts.org

Appendix A: Security Breach Risk Assessment Checklist

A. What is the nature of the breach?
   (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)
B. How did the breach occur?
C. What type of Data is involved?
   (The individual data fields should be identified e.g. name, address, bank account number, commercially sensitive contracts)
D. How many individuals or records are involved?
E. If the breach involved personal data, who are the individuals?
   (Delegates, members, committee etc.)?
F. What has happened to the data?
G. Establish a timeline?
   (when did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc.)
H. Were there any protections in place? (e.g. encryption)
I. What are the potential adverse consequences for individuals or the BTS? How serious or substantial are they and how likely are they to occur?
J. What could the data tell a third party about an individual, what harm could this cause? What commercial value does the information have?
K. What processes/systems are affected and how?
   (e.g. web page taken off line, access to database restricted)

Appendix B:
Notification of breach checklist - who to notify

There should be a purpose to notifying individuals of a breach, it may be that there are steps they need to take to protect themselves, BTS may be legally or contractually obliged to report breaches to stakeholders or we may need to manage potential reputational damage. The following (non-exhaustive) list identifies key external stakeholders who may require notification.

- BTS President and Data Protection Officer – in all circumstances
- Police – in the case of criminal activity
- Individuals whose data has been compromised
- Information Commissioner's Office (ICO)
- Regulatory bodies
- Others – e.g. banks where steps may be required to protect accounts

The data protection officer should advise on the content of any message sent. Any notification message should not be sent too quickly, it is important that the extent of the breach is understood fully and BTS are able to provide useful information, whilst at the same time if there are important steps that individuals need to take this should be communicated promptly. The only exception is the requirement to inform the relevant governing body within the current legislative time frame, this must be adhered to.

In any message, you should consider including the following:

- Details of what happened and when the breach occurred
- What data was involved
- What steps have been taken to contain the breach and prevent reoccurrence
- Advice on what steps they should take e.g. contact banks
- How will you help and keep them informed (if necessary)
- Provide a way to be contacted

Appendix C:

Data Breach Activity Log

Data breach date:	
Data breach description:	
Person responsible for handling data breach:	

ACTION TAKEN	**DATE**