Victorguard Care

POLICY NO: 107-2

PERSONAL DATA BREACH POLICY

1. POLICY DETAILS

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- ✓ access by an unauthorised third party;
- ✓ deliberate or accidental action (or inaction) by a controller or processor;
- ✓ sending personal data to an incorrect recipient;
- ✓ computing devices containing personal data being lost or stolen;
- ✓ alteration of personal data without permission; and
- ✓ loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

When a personal data breach has occurred, The Data Protection Officer will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then DPO notify the ICO. However, if DPO decide not to report the breach, explanation of that decision will be done as a part of case documentation.

2. NOTIFICATION TO THE SUPERVISORY AUTHORITY

DPO will report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If it takes longer than this, the reasons for the delay must be documented.

When reporting a breach following information must be provided must provide:

- a description of 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 (if your organisation has one) or other contact point where more information can be obtained;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

To report the beach, please follow the instruction on website linked below:

https://ico.org.uk/for-organisations/report-a-breach/

Remember, in the case of a breach affecting individuals in different EU countries, the ICO may not be the lead supervisory authority. This means that as part of your breach response plan, you should establish which European data protection agency would be your lead supervisory authority for the processing activities that have been subject to the breach. For more guidance on determining who your lead authority is, please see the Article 29 Working Party.

3. NOTIFICATION TO THE INDIVIDUAL

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.

Notification to the individual is expected to cover following aspect:

- the name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

4. OTHER STEPS IN RESPONSE TO THE BREACH

DPO will ensure that all breaches are recorded, regardless of whether or not they need to be reported to the ICO.

Article 33(5) requires you to document the facts relating to the breach, its effects and the remedial action taken. This is part of the overall obligation to comply with the accountability principle and allows to verify the organisation's compliance with its notification duties under the GDPR.

As with any security incident, we will investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

Policy date: ……..

Authorised signatory: ……..

Policy revive date: ……..