Within 12 hours of becoming aware of the breach:
- Notify IIPCIC Senior Management: Nature of the breach; assessment of risk; recommended response.
- Containment and recovery: Stop breach, understand how occurred; start creation of recovery plan, damage limitation, who to lead our response, risk to individuals (internal and external):
- See ICO best practice on breach management

Within 24 hours of becoming aware of the breach:
- Where the breach affects our clients/customers personal data – notify them of the breach.

Within 72 hours of breach:
- Within 72 hours report to ICO: Include details of the security measures in place e.g encryption and details of the security procedures at the time of breach. Also, are media aware of the breach or likely to be?

Decision: Does breach need reporting to ICO?
- Yes

Decision: Do affected individuals need to be informed?
- Yes

Within 72 hours of breach:
- Give specific and clear advice on the steps they can take to protect themselves and also what we will do to help. Provide a way in which they can contact us for further information or ask questions.

Within 72 hours of breach:
- Implement data breach recovery plan

Within four days of breach:
- Compile a comprehensive report to summarise the nature of the breach, steps taken to date to mitigate, inform etc and steps still to be taken

Within one week of breach:
- Key recommendations made to senior management to review the organisation’s response to the breach, lessons learned, and any new procedures/security measures implemented

Data security breach managed

Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, the GDPR requires that the controller shall notify the breach to the ICO without undue delay and, where feasible, not later than 72 hours after having become aware of it. A controller should be regarded as having become “aware” when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.