Information Security Incident Reporting

Introduction

Information security is everyone's responsibility; these guidelines have been developed to assist Horizon Strategic Partners employees to identify security incidents, suspected security weaknesses or near misses, security threats to services or systems and how to report these incidents through appropriate management channels.

An Information Security Incident

An information security incident is any violation of Horizon Strategic Partners Information Governance (IG) Policy. The term security incident and suspected incidents is very broad and includes, but not limited to, incidents that effect disclosure, denial of access to, destruction or modification of Horizon Strategic Partners data.

Examples of security incidents:

- Using another user's login id
- Unauthorised disclosure of information
- Leaving confidential / sensitive files out
- Theft of IT equipment
- Accessing a persons record inappropriately e.g. viewing your own health record or family members, neighbours, friend etc.,
- Writing passwords down

Diligent employees should question procedures, protocols and events that they consider could cause damage, harm, distress, break of compliance or bring Horizon Strategic Partners into disrepute.

Reporting of Security Incidents

All security incidents should be reported to the IG Lead**;** incidents will be recorded on YouTrack. All security breaches will be forwarded to the IG team, who will log the event on the organisations risk register PRISM, investigate, document and feedback. All incidents will be monitored, to identify recurring or high impact incidents. This may indicate the need for enhanced or additional controls.

By reporting incidents it allows the organisation to relate to similar occurrences and highlights any areas of vulnerability, identifying where greater awareness is needed, or procedures/ protocols that require reviewing. Good reporting generates better statistical data thus, keeping the organisation informed.

When reporting a security incident, it is important to ensure sufficient information is given to the IG Lead to enable them to understand and respond appropriately to the

report. Users can report security related incidents in confidence, no information about a user's involvement in a security incident will be released without explicit permission.

If reporting software malfunctions, symptoms of the problem and any messages appearing on the screen should be noted. The PC should be isolated and the use of it stopped, until reported. Users must not attempt to remove suspected software or attempt to 'repair/mend' equipment unless authorised to do so.

Description of Incident

It is important that security incident reports give as much detail as possible. Including a description of activities leading up to the security incident, information about circumstances prevailing at the time, how the incident came about, how the security incident was detected.

The security incident or suspected security incident report where possible should not include personal identifiable information. This will not always be possible as to exclude a persons name i.e. in the case of theft, Fred Smith's laptop has been stolen from his desk, would be meaningless reported as; *a laptop has been stolen from a desk*.

Whenever possible when reporting security incidents, relate them to the protocols or procedures that may have been compromised. An audit report can be a useful document, providing background to security incidents.

All security incidents will be prioritised to the seriousness of the incident by the IG team.

The Horizon Strategic Partners IS Policy requires that security incidents be reported as soon as possible to the event being identified. Reports sent immediately after the incidents are likely to be the most valuable, if there is a delay between an incident occurring and the discovery of said incident, the incident should still be reported.