PRODATA
consulting | systeme | services

IT Security Incident Reporting and Response Policy

1 PURPOSE

This policy governs the actions required for reporting or responding to security incidents involving PRODATA information and/or information technology resources to ensure effective and consistent reporting and handling of such events.

2 DEFINITION SECURITY INCIDENT

Any real or suspected event that may adversely affect the security of information or the systems that process, store, or transmit that information. Examples include:

- Unauthorized access to data, especially confidential data like a person's name and address
- Computer infected with malware such as a worm, virus, Trojan Horse, or botnet
- Reconnaissance activities such as scanning the network for security vulnerabilities
- Denial of Service attack
- Web site defacement
- Violation of a PRODATA security policy
- Security weakness such as an un-patched vulnerability

3 POLICY

3.1 Reporting Security incidents

All suspected incidents must be reported to the Managing Director

3.2 Responding to Security Incidents

3.2.1 Incident Severity

Incident response will be managed based on the level of severity of the incident. The level of severity is a measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response. Four levels of incident severity will be used to guide incident response: high, medium, low, and NA (Not Applicable).

- High

  The severity of a security incident will be considered "high" if any of the following conditions exist:

  1. Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire institution is affected)
  2. Poses a potential large financial risk or legal liability to the Company
  3. Threatens confidential data (for example, the compromise of a server that contains or names with social security numbers or credit card information)
  4. Adversely impacts an enterprise system or service critical to the operation of a major portion of the company
  5. Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.
  6. Has a high probability of propagating to many other systems inside and/or outside PRODATA and causing significant damage or disruption

- Medium

  The severity of a security incident will be considered "medium" if any of the following conditions exist:

  1. Adversely impacts a moderate number of systems and/or people
  2. Adversely impacts a non-critical enterprise system or service
  3. Adversely impacts a departmental system or service, such as a departmental file server
  4. Disrupts a departmental network
  5. Has a moderate probability of propagating to other systems inside and/or outside PRODATA and causing moderate damage or disruption

- Low

  Low severity incidents have the following characteristics:

  1. Adversely impacts a very small number of systems or individuals
  2. Disrupts a very small number of network devices or segments
  3. Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate

- NA (Not Applicable)

  This is used for events reported as a suspected IT security incident but upon investigation of the suspicious activity, no evidence of a security incident is found

3.2.2 Incident Response

Required handling of IT security incidents based on incident severity

- High

  Response Time: Immediate
  Incident Manager: Executive Incident Management Team
  Who to Notify: Managing Director
  Post-Incident Report Required: yes

- Medium

  Response Time: 4 hours
  Incident Manager: Appointed by Management
  Who to Notify: Managing Director
  Post-Incident Report Required: No, unless requested by Managing Director

- Low

  Response Time: Next 3 business days
  Incident Manager: Technical administration
  Who to Notify: Managing Director
  Post-Incident Report Required: No

- NA (Not Applicable)
  This is used for events reported as a suspected IT security incident but upon investigation of the suspicious activity, no evidence of a security incident is found

3.3 Media incident Information policy

A high incident may generate media interest, which must be handled in accordance with this policy. The media will seek accurate, regular and timely information, accessible through a variety of channels.

All media requests for information will be handled only by the Managing Director who will be responsible for issuing statements, arranging spokespeople and, if appropriate, organising media briefings.