Definitions of Incident Severity:

I. **Critical** – This category of incident may have a severe impact to your network or system and indicates a compromise. Examples of incidents that fall under this category: malware infection, backdoor or Trojan traffic, outbound DDoS, and bot net traffic.

II. **High** – This category of incident may have a high impact on your network or system and could lead to malware infection, data leakage, and disruption of operations due to network or system down time. Examples of incidents that fall under this category: download of malicious software, leakage of file from internal network, DoS or DDoS, P2P traffic (torrent), cloud storage traffic, and exploit launching.

III. **Medium** – This category of incident has a medium level of impact on your network or system and could lead to unnecessary leakage of information or exposure of vulnerabilities. Examples of incidents that fall under this category: port scans, vulnerability scans, social media traffic, unusual network traffic, and multiple failed logins.

IV. **Low** – This category of incident shows little impact on the Customer. This is mostly informational alerts to inform the Customer. Examples of incidents that fall under this category: login or logout notifications, failed login notifications, application or system update notification, and application or system error message.

V. **Informational** – This category of incident shows no impact to the Customer. This is only informational alerts to track activity. Examples of incidents that fall under this category: false positives, approved scanning vendors, and test alerts.