UNSC GWG

Global Platform of Data, Services and Applications (GP)

Incident Management

1. Incident Management

| Ref | Description | Type | Priority |
| --- | --- | --- | --- |
|  | The Supplier MUST clearly define and communicate what they consider incidents (such as data breaches) versus mere events (such as suspicious intrusion detection alerts). | Non-functional | Must Have |
|  | The Supplier MUST detail the communication paths to the incident response teams. | Non-functional | Must Have |
|  | The Supplier MUST support an incident management process to alert the customer in near real time to high risk threats or issues that have arisen that may have or may in future compromise service / data confidentiality, integrity or availability, and provides customer with updates on mitigations taken.  This includes security breaches or other adverse events that have affected other customers or shared service elements, whether or not they have adversely affected contracting authority services at that time. | Non-functional | Must Have |
|  | The Supplier MUST provide details of the hours of support | Non-functional | Must Have |
|  | The Supplier MUST provide details of the maximum time the Supplier will take to acknowledge an inquiry or request, along with the details of the severities. | Non-functional | Must Have |
|  | The Supplier MUST provide details of the maximum target resolution time the Supplier will take to acknowledge an inquiry or request, along with the details of the severities. | Non-functional | Must Have |
|  | The Supplier SHOULD provide a forensic image if required | Non-functional | Should Have |
|  | The Supplier MUST accept a contractual commitment to assist with forensics requests in the event of a data breach. | Non-functional | Must Have |