**Service Level Agreement – SLA**

**IT-säkerhet**

**för**

**Säkerhetsteknik 2020**

**Mall**

**2021 08 13**

**Version:**

**Version:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Datum** | **Revision/beskrivning** | **Författare** | **Övrig information** |
| 1.1 | 2021-08-13 |  |  | mall |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Godkänd av**

|  |  |  |  |
| --- | --- | --- | --- |
| **Part** | **Namn** | **Titel** | **Datum** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Incidentrapportering

Leverantören skall notifiera beställare om säkerhetsincidenter senast 72 timmar efter att Leverantören blivit medveten om incidenten.

Leverantören skall meddela information gällande inträffad säkerhetsincident och skall innefatta en beskrivning av incidenten, status för leverantörens utredning och mitigering samt den potentiella skada och/eller påverkan denna incident har på beställaren.

I det fall incidenten inkluderar personuppgifter skall samtliga relevanta regler för GDPR följas.

Sårbarheter

Sårbarheter skall som princip fixas så fort som möjligt. För kritiska (Critical & High) sårbarheter där det finns en tydlig risk för exploatering skall en fix eller en mitigerande åtgärd vara på plats senast 7 dagar efter att sårbarheten blivit känd. För mindre kritiska (Medium) sårbarheter skall en fix vara införd och/eller mitigerande åtgärder implementerade inom 30 dagar från att sårbarheten blivit känd.

För att erhålla en tydlighet i definition av sårbarhet nyttjas CVSS scoring för att definiera en sårbarhet.



Om ingen uppdatering är tillgänglig eller lämplig motåtgärd saknas, bör andra säkerhetsåtgärder övervägas, såsom att:

1. stänga av tjänster eller funktioner relaterade till sårbarheten
2. anpassa eller lägga till säkerhetsåtgärder för att minimera den aktuella sårbarheten
3. utöka övervakningen för att upptäcka verkliga attacker genom utökad loggning i SIEM eller brandvägg
4. öka medvetenheten om sårbarheten för att minimera att en lyckad attack skall kunna genomföras.

Patch management

Patchar skall följa leverantörens rekommendationer. Detta gäller för buggfixar samt säkerhetsuppdateringar. Exempelvis skall Leverantören 7 dagar efter ”patch Tuesday” starta utrullning av senaste patcharna för Microsoft Windows, om applicerbart. Processen för ändringshantering skall dock nyttjas och samtliga förändringar i miljön skall vara analyserade, verifierade och testade innan de införs.