Security Incident Response Handbook Feedback

Introduction

The Security Incident Response Handbook for the eduGAIN service has been developed by the REFEDS Sirtfi Working Group in collaboration with the eduGAIN Security Team. The document defines the roles and responsibilities of each party taking part in the Security Incident Response process that is when a Federation Participant suspects a security incident affects its resources and has reason to believe that Federation Participants outside its origin federation may be affected. The groups are now seeking feedback on this document.

The document has been already extensively commented by both the REFEDS and eduGAIN community during a public consultation last year, which lead to many changes and amendments to the original document. The current version has been fully endorsed by the REFEDS Steering Commitee and it is now presented to the eduGAIN Steering Group for adoption and incorporation into the current eduGAIN policy set.

Feedback

We invite you to add comments and change proposals for the adoption of the current Security Incident Response Handbook. Please use this Line numbered PDF version of the document.

Change Log

<table>
<thead>
<tr>
<th>Line Number / Reference</th>
<th>Comment or change proposal</th>
<th>Proposer / Affiliation</th>
<th>Action / Decision (please leave blank)</th>
</tr>
</thead>
</table>
| 162-165                 | The process described in item 10 is ambiguous and could be misinterpreted to imply a wider distribution of the lessons learned document, and also to not distribute it to organisation which use TLP without full SIRTFI. I therefore suggest the current paragraph is replaced with:  
“In collaboration with your Federation Operator, produce a report of the incident labelled with TLP:AMBER or higher which includes lessons learned and actions taken, and share to affected organisations in all federations which are SIRTFI-compliant or that support the TLP, within one month of resolution of the incident.” | Alex Stuart (Jisc) |                                           |
| 194-197                 | Change wording of item 8 in Federation Operators’ procedures to match that in item 10 of the Federation Participants’ procedures, as in the previous change proposal. | Alex Stuart (Jisc) |                                           |