○ 자가점검체크리스트

- 증빙자료에서 각 항목 검토기준을 충족하는 내용은 모두 발췌하여 자가점검체크리스트 증빙내용에 기재하여야 이를 검토할 수 있음

※ 자가점검체크리스트도 해당 서비스에 대한 검토를 하는 자료이므로, 증빙자료에서 검토기준에 해당하는 내용은 모두 발췌하여 작성해야 검토가 가능함

- 1.2~3.2 각 항목의 증빙 문서명에는 기존에 적시되어 있는 내용은 삭제하고 해당 항목 증빙 내용에 기재한 내용을 발췌한 증빙자료명을 기재 필요

○ 디지털서비스 공급 및 기술지원 확약서

- 엔에이치엔클라우드의 발급본의 원 제공자명은 엔에이치엔과 클라우드 사이 공백이 없어야 하며, 뒷면의 역할 구분 명세서 중 지원체계 항목에 이용자 지원체계 제시 부분은 원 제공자와 중개 제공자가 모두 부의 역할을 담당하는 것으로 기재되어 있음, 수정 필요

※ 디지털서비스 공급 및 기술지원 확약서 내 역할 구분 명세서에 기재된 역할에 맞게 증빙자료가 제출되어야 하며, 다를 경우 해당 서비스에 대한 검토가 불가하니 참조하여 자가점검체크리스트 증빙내용 및 증빙자료를 수정

○ 제공역량

1.2 침해사고 대응 절차 및 사후관리 대책

□ 자가점검체크리스트 증빙내용 및 증빙자료의 내용이 침해사고 대응절차 및 사후관리 대책의 적정성을 충족하는 내용으로 검토하기에 미흡함

- 침해사고 대응절차도에 있는 개인정보취급자, 개인정보보호 담당자/책임자, 침해사고처리 대응팀/책임자, 최고책임자는 신청사(아이티아이즈)의 내부 조직일텐데, 이 조직이 어떻게 구성되어 있는지에 대한 내용이 없이는 이를 내부 절차도로 확인할 수 없음

- 또한, 증빙자료에서 제시된 절차도와 그 뒤에 상황별 대처하는 내용이 전혀 매칭이 되지 않음, 절차도에 따라 처리되는 내용이 확인이 되어야 하는데, 내용은 보완의견 받기 전 내용을 제시하고 이와 전혀 상관없는 절차도를 제시하면 무슨 내용을 검토해야 할지 모르겠음

- 물적보안, 인적보안과 관련된 내용이 기재된 자료가 지난번에는 있었으나 이번 제출에서는 누락됨(00.정보보호 정책서\_Ver0.1.pdf)

- 물적보안, 인적보안으로 제시된 내용은 증빙자료에서 확인할 수 없음

- 주기적인 훈련 및 점검실시 계획과 관련된 내용은 여전히 증빙자료에서 누락되어 확인할 수 없음

※ 1차, 2차 보완때마다 어떤 부분이 반영이 되면, 기존 반영되어 있던 부분이 누락되는 부분이 다수 확인됨

1.3 개인정보·데이터 관리정책

□ 데이터 처리위치 및 국외이전여부로 제시된 내용을 통해 국외 이전 여부는 확인이 되나 개인정보, 데이터 처리 위치의 내용은 확인할 수 없음

- 적시된 내용은 각 원 제공자들이 수집하는 항목과 시점만 제시될 뿐 이를 어디서 처리되는 위치는 제시되지 않음

※ 지난 보완요청 당시 의견이 반영되지 않았으며, 원 제공자가 데이터를 처리하면 그 위치가 어디인지에 대한 내용이 제시되어야 하는데, 제시된 내용으로는 그러한 내용을 확인할 수 없음

※ 1차, 2차 보완 모두 의견이 전달되었으나, 반영되지 않음, 검토기준을 충족하는 내용으로 제시되어야 서비스 검토가 가능한 부분을 참고하여 서비스 신청 진행 필요

1.4 안전한 코딩방법

□ 제시된 점검도구나 점검 절차를 통해 이러한 시큐어코딩 점검/조치를 진행하는 내용을 수행한 증빙자료가 제시되어 이를 확인해 이를 수행할 역량을 갖추고 있음으로 검토하는데, 현재는 이를 점검/조치한 내역은 확인할 수 없음

- 이러한 도구나 절차를 통해 수행한 내역이 같이 확인되어야 이를 수행할 역량을 갖추고 있음으로 검토하는 점 참고 필요

1.5 취약점 점검 및 조치

□ 제시된 점검도구나 점검 절차를 통해 이러한 취약점 점검/조치를 진행하는 내용을 수행한 증빙자료가 제시되어 이를 확인해 이를 수행할 역량을 갖추고 있음으로 검토하는데, 현재는 이를 점검/조치한 내역은 확인할 수 없음

- 이러한 도구나 절차를 통해 수행한 내역이 같이 확인되어야 이를 수행할 역량을 갖추고 있음으로 검토하는 점 참고 필요

2.1 가용률

□ 증빙자료는 해당 원 제공자의 가용률 정책을 확인할 수 있는 원 자료를 그대로 제출 필요(지금은 보장정책만 확인할 수 있는 내용만 캡쳐해 자료로 제출됨)

- 보장정책만 캡쳐된 자료로 이를 원 제공자의 정책이라고 검토하기에는 미흡함

□ 공급 및 기술지원 확약서에서 중개 제공자는 해당없음으로 제시했으므로, 신청사(아이티아이즈)의 가용률 내용은 삭제

※ 서비스를 신청하는 입장에서는 어떤 원 제공자의 정책이라고 확인할 수 있으나 보장정책만으로 이 정책이 어떤 원 제공자의 정책인지 이를 검토하는 위원은 확인할 수 없음

2.2 모니터링 정보

□ 검토기준을 확인하고 해당 검토기준에 맞는 내용을 발췌해서 자가점검체크리스트 증빙내용에 기재해야 할 필요가 있음

- KT의 경우 모니터링 정보 제공주기와 제공 방법 항목은 모니터링 정보를 어떤 주기로 제공하고 이를 어떤 방법으로 제공하는지에 대한 내용이 제시되어야 하지만 해당 부분에 Watch API 내용을 기재해두어, 맞지 않은 내용이 제시된 것으로 확인됨

□ 공급 및 기술지원 확약서에서 중개 제공자는 해당없음으로 제시했으므로, 신청사(아이티아이즈)의 모니터링 내용은 삭제

2.3 백업 및 복구

□ 공급 및 기술지원 확약서 내 역할 구분 명세서에서 지원하는 원 제공자에 따라 장애대응체계 항목에 대한 역할이 상이함(네이버, NHN클라우드는 원 제공자 정/중개 제공자 부의 역할을 담당하지만, KT클라우드는 원 제공자 정/중개 제공자 해당없음의 역할을 담당함)

- 자가점검체크리스트에는 KT클라우드의 장애대응체계만 확인되고, 네이버나 NHN의 장애대응체계는 확인되지 않음(네이버나 NHN도 결국 정의 역할을 하므로 정의 역할을 하는 내용이 증빙자료나 자가점검체크리스트에 기재되어야 함)

- 원 제공자 정, 중개 제공자 부의 역할을 하는 내용으로 검토하려면 원 제공자가 정의 역할을 하는 내용과 중개 제공자가 원 제공자의 정 역할을 뒷받침하는 부의 역할을 하는 내용도 같이 제시되어야 할 것으로 사료됨

□ 공급 및 기술지원 확약서 내 역할 구분 명세서에서 지원하는 원 제공자에 따라 백업정책 항목에 대한 역할이 상이함(NHN클라우드는 원 제공자 정/중개 제공자 부의 역할을 담당하지만, 네이버, KT클라우드는 원 제공자 정/중개 제공자 해당없음의 역할을 담당함)

- NHN클라우드에 대한 중개 제공자가 부의 역할을 하는 내용은 확인할 수 없음

※ 상식적으로 원 제공자는 다르더라도 운영안정성 장애대응체계나 백업 및 복구는 원 제공자의 정책을 준용할 것으로 사료되며, 그렇다면 공급 및 기술지원확약서에도 그 제공자는 다르나 준용하는 내용으로 동일하게 체크되어야 하므로, 확인 하여 획일화 된 내용으로 확인할 수 있게 체 크 후 제출 필요

3.1 조직·인력 구성 현황 및 이용자 지원 체계

□ 조직인력 구성현황과 이용자 지원체계 중 네이버클라우드의 이용자 지원체계의 내용만 자가점검체크리스트 증빙내용에 기재되어 있음

□ 이용자 지원체계로 어떤 내용을 제시하는지에 대한 설명을 추가해 제시해야하는데, 그러한 내용없이 자료만 제시하는 것으로 무슨 내용인지 파악하기에는 미흡함

□ 클라우드 지원서비스 조직역량에 해당하는 인력이나 수행실적은 확인이 되었으나 다시 제출된 자가점검체크리스트 에서는 누락되었고, 여전히 실제 지원서비스를 수행하는 방법론에 대한 내용은 자가점검체크리스트 증빙내용에서도 누락되었고, 증빙자료에서도 확인되지 않음

□ 공급 및 기술지원 확약서 내 역할 구분 명세서 내 이용자 지원체계는 중개 제공자인 아이티아이즈가 정, 원 제공자가 부의 역할을 수행하는것으로 기재되어 있는데, 제시된 내용을 통해서는 이러한 역할을 담당하는것으로 확인할 수 없음

- 중개 제공자가 정, 원 제공자가 부의 역할을 하는것으로 체크되었으나, 제시된 자료에는 원 제공자가 정, 중개 제공자는 해당없음의 내용으로 확인되어 동일한 내용으로 검토할 수 없음

제출 내용이 미흡하여 반려되었으니 상기 보완 내용 참고 부탁드립니다. 기타 문의사항은 053-214-7458(심용민 선임연구원)으로 연락주시면 피드백 드리겠습니다.