NIA 한국지능정보사회진흥원

디지털서비스 심사·선정기준 안내

목차

NIA 한국지능정보사회진흥원

01 심사선정절차

1. 심사신청·접수

서류 확인

2. 전문가 검토

검토 의견서, 검토 결과보고서

*필요시 현장실사 및 기업면담 실시+

3. 심사위원회 심사

디지털서비스 선정

4. 디지털서비스 선정

선정 통보서 발급

02 심사신청 및 접수

01 공통서류

02 클라우드컴퓨팅 제출서류

공통서류

- 디지털서비스 심사 신청서
- 법인 등기사항전부증명서
- 사업자등록증
- 신용평가등급확인서
- 디지털서비스개요서
- 디지털서비스 제공역량 증명자료

클라우드컴퓨팅 제출서류

- 클라우드 보안 인증제 인증서

  각급 학교에 학생들의 교육 목적으로 제공하는 클라우드컴퓨팅서비스는 예외+

  ※ 클라우드 보안인증서 제출 시 보안성 관련 심사 항목 생략
- 서비스 수준 정책서
- 디지털서비스 원 제공자의 공급 및 기술지원 확약서
- 디지털서비스 원 제공자-중개 제공자 간 제공 역량 항목별 구분 명세서+

03 디지털 서비스 검토 기준

디지털 서비스 해당여부

경영상태 (적격성)

제공역량

1. 디지털서비스 해당여부

1.1 클라우드 컴퓨팅서비스

1.2 클라우드 지원서비스(컨설팅, 운영관리, 마이그레이션,기타)

1.3 융합서비스(다른 기술 · 서비스가 융합된 서비스)

2. 경영상태(적격성)

2.1 경영상태

① 신용평가등급 B- 미만인 경우(창업 3년 이내 기업 면제)

② 휴·폐업, 부도 또는 파산상태로 해당 계약 이행이 불투명

(단, 회생계획인가결정 등 법원 정상화 판결을 받은 경우 제외)

2.2 부정당업자 제재 여부 신청일 기준으로 부정당업자 제재 중인 자

3. 제공역량

3.1 보안성

3.2 운영안정성(가용률, 모니터링 정보, 백업 및 복구)

3.3 지원체계(이용자 지원체계, 고객 대응 관리체계)

04 제공 역량

보안성

검토 항목

1. 보안성

1.1 클라우드 보안인증제에 따른 인증서 제출

- 클라우드컴퓨팅서비스에 한하며, 각급 학교에 학생들의 교육목적으로 제공하는 클라우드 컴퓨팅서비스 임을 [별지 제6호 서식]에 따라 제출한 경우에는 예외+

※ 클라우드 보안인증제에 따른 인증서 제출 시에는 1.2~1.5 항목 검토 생략

1.2 침해사고 대응 절차 및 사후관리대책

1.3 개인정보·데이터 관리정책

1.4 안전한 코딩방법

1.5 취약점 점검 및 조치

04 제공 역량

보안성 침해사고 대응 절차 및 사후관리 대책

검토 항목

검토 내용

검토 기준

1.1 클라우드 보안인증제에 따른 인증서 제출

클라우드 보안인증서를 제출하였는가?

- **클라우드컴퓨팅서비스에 한하여 반드시 제출**
  - 클라우드 보안인증서 제출 시에는 1.2~1.5 항목 검토 생략

※ 각급 학교에 학생들의 교육 목적으로 제공하는 클라우드컴퓨팅서비스는 예외+

04 제공 역량

보안성 침해사고 대응 절차 및 사후관리 대책

검토 항목

검토 내용

검토 기준

1.2 침해사고 대응 절차 및 사후관리대책(1/2)

클라우드컴퓨팅법, 정보통신망법 등 관련 법률에서 침해사고와 관련하여 요구하는 준수사항으로

1) 침해사고 발생시 이용자에게 **“통지의 내용 및 방법”을 명시하여 제시하고 있는가?**

- **“침해사고 통지 내용 및 방법”의 적정성**

– 침해사고 통지 방법, 침해사고 발생 내용, 발생원인, 서비스 제공자의 피해확산 방지 조치 현황, 서비스 이용자의 피해 예방 또는 확산방지 방법, 담당부서 및 연락처 등을 포함하여 제시

04 제공 역량

보안성 침해사고 대응 절차 및 사후관리 대책

검토 항목

검토 내용

검토 기준

1.2 침해사고 대응 절차 및 사후관리대책(2/2)

클라우드컴퓨팅법, 정보통신망법 등 관련 법률에서 침해사고와 관련하여 요구하는 준수사항으로

2) 침해사고에 효과적으로 **대응하고 재발을 방지하기 위한 절차가 있는가?**

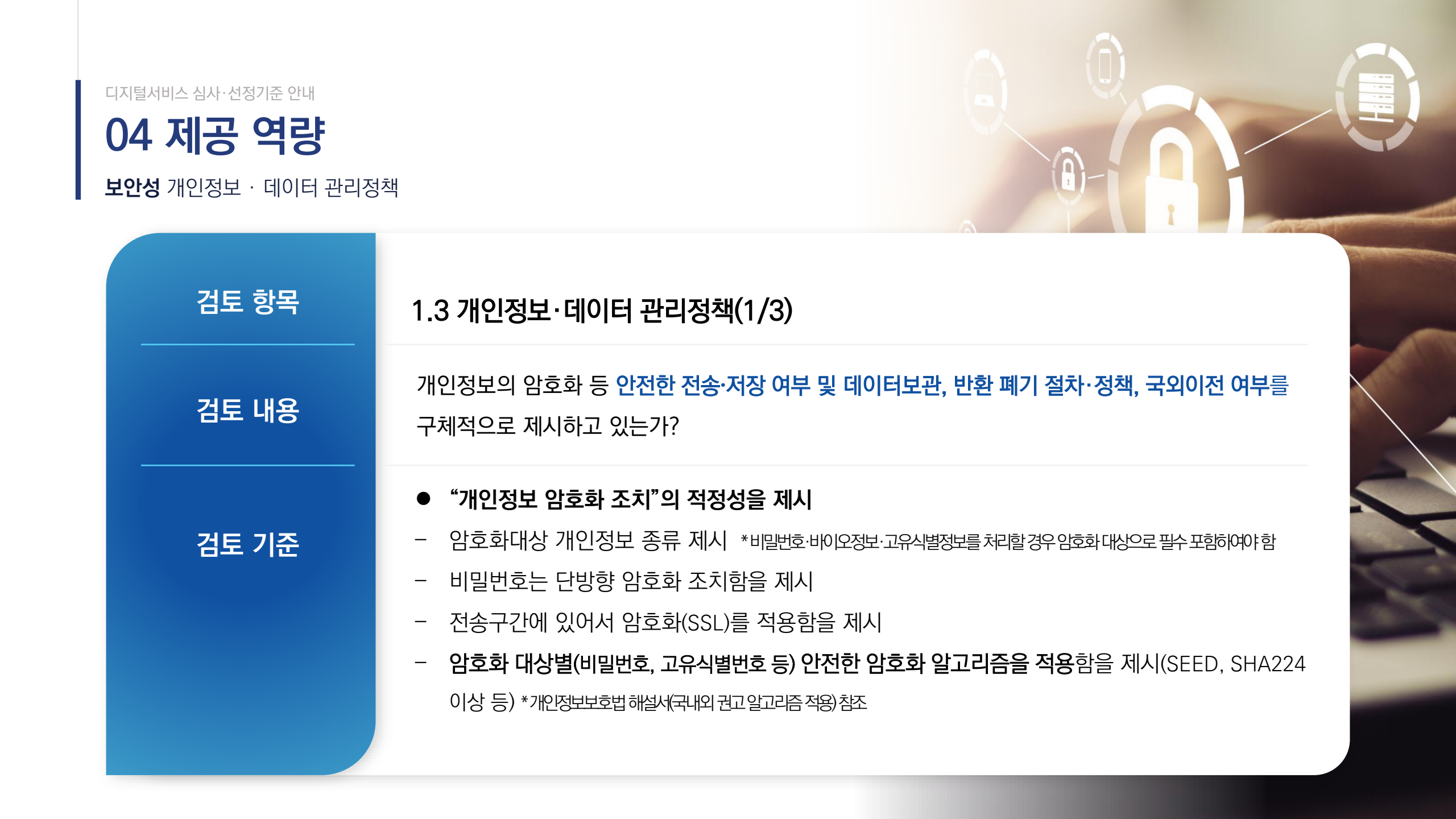
- **“침해사고 대응 절차 및 사후관리 대책”의 적정성**

– 침해사고 원인분석 및 대응 절차, 재발 및 확산방지 대책, 주기적인 훈련 및 점검 실시 계획 등을 포함하여 제시

* 재발 및 확산방지 대책으로는 시스템 개선사항 및 보안교육 실시계획 등을 포함할 수 있음

04 제공 역량

보안성 개인정보 · 데이터 관리정책



검토 항목

검토 내용

검토 기준

1.3 개인정보·데이터 관리정책(1/3)

개인정보의 암호화 등 **안전한 전송·저장 여부 및 데이터보관, 반환 폐기 절차·정책, 국외이전 여부**를 구체적으로 제시하고 있는가?

- **“개인정보 암호화 조치”의 적정성을 제시**
  - 암호화대상 개인정보 종류 제시 *비밀번호·바이오정보·고유식별정보를 처리할 경우 암호화 대상으로 필수 포함하여야 함
  - 비밀번호는 단방향 암호화 조치함을 제시
  - 전송구간에 있어서 암호화(SSL)를 적용함을 제시
  - **암호화 대상별(비밀번호, 고유식별번호 등) 안전한 암호화 알고리즘을 적용**함을 제시(SEED, SHA224 이상 등) *개인정보보호법 해설서(국내외 권고 알고리즘 적용) 참조

04 제공 역량

보안성 개인정보 · 데이터 관리정책

검토 항목

검토 내용

검토 기준

1.3 개인정보·데이터 관리정책(2/3)

개인정보의 암호화 등 안전한 전송·저장 여부 및 데이터보관, 반환 폐기 절차·정책, 국외이전 여부를 구체적으로 제시하고 있는가?

● **“데이터 반환 및 폐기 절차”의 적정성**

– 데이터 반환 및 폐기 절차, **데이터 국외이전 여부, 데이터·서비스 처리 위치(국내/국외) 포함**하여 제시

※ 개인정보를 처리하지 않거나 암호화 대상이 없을 경우 개인정보 처리하지 않고 있음과 암호화 대상여부가 없음을 반드시 명시

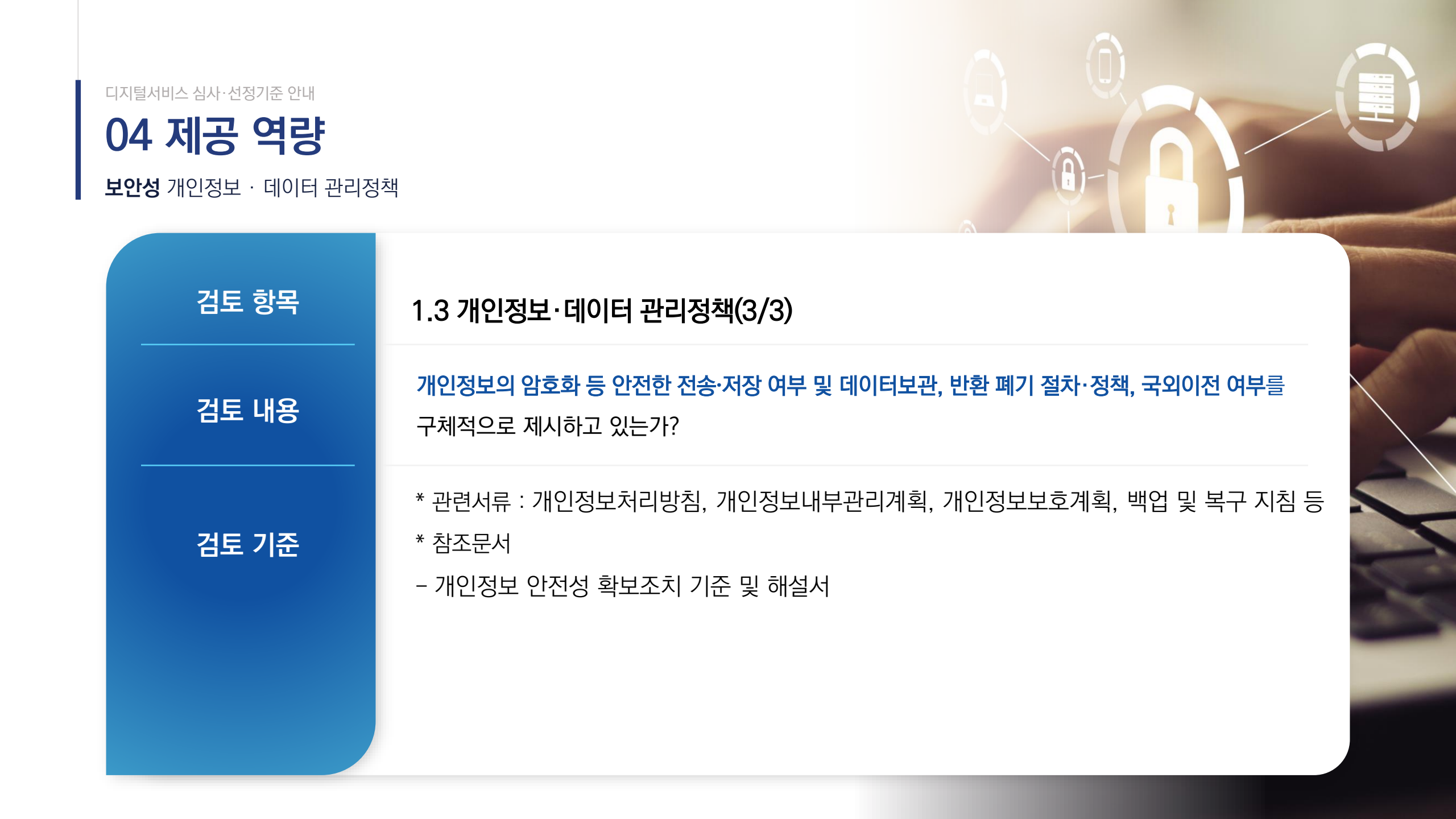
※ “처리”란 개인정보 및 데이타의수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 의미

* 관련서류 : 개인정보처리방침, 개인정보내부관리계획, 개인정보보호계획, 백업 및 복구 지침 등

* 참조문서 : 개인정보 안전성 확보조치 기준 및 해설서

04 제공 역량

보안성 개인정보 · 데이터 관리정책



검토 항목

검토 내용

검토 기준

1.3 개인정보·데이터 관리정책(3/3)

개인정보의 암호화 등 안전한 전송·저장 여부 및 데이터보관, 반환 폐기 절차·정책, 국외이전 여부를 구체적으로 제시하고 있는가?

* 관련서류 : 개인정보처리방침, 개인정보내부관리계획, 개인정보보호계획, 백업 및 복구 지침 등
* 참조문서
- 개인정보 안전성 확보조치 기준 및 해설서

04 제공 역량

보안성 안전한 코딩방법

검토 항목

검토 내용

검토 기준

1.4 안전한 코딩방법(1/2)

안전한 코딩방법에 따라 구현될 수 있는지 확인할 수 있는 **점검방법과 점검절차 등 점검체계를 제시**하고 있는가?

- **시큐어코딩 점검계획 수립 여부 및 그 내용의 적정성 확인**
  - **점검방법(수행주체, 점검 툴 등 포함), 점검시기, 점검결과에 따른 조치사항** 등을 포함하여 제시

* 별도의 점검 툴 없이 전문인력을 활용할 경우에는 해당 내용을 명기

* 다만, 기술적 보안 취약점 점검에 있어서 신청한 서비스 특성 및 운영 상황을 고려하여 적합한 점검방법 및 점검기준을 적용

04 제공 역량

보안성 안전한 코딩방법

검토 항목

검토 내용

검토 기준

1.4 안전한 코딩방법(2/2)

안전한 코딩방법에 따라 구현될 수 있는지 확인할 수 있는 **점검방법과 점검절차 등 점검체계를 제시**하고 있는가?

* 관련서류 : 정보보호정책서, SW개발보안지침, 점검계획서 및 조치 결과보고서 등 결재 문서

* 참조 문서

- 소프트웨어 개발보안 가이드(행정안전부, 2019.11.)
- 소프트웨어 보안약점 진단가이드(행정안전부, 2019.6.)
- 공개소프트웨어를 활용한 소프트웨어 개발보안 진단 가이드(행정안전부, 2019.6.)
- https://www.kisa.or.kr/public/laws/laws3.jsp 참조

04 제공 역량

보안성 취약점 점검 및 조치

검토 항목

검토 내용

검토 기준

1.5 취약점 점검 및 조치(1/2)

서비스 SW 및 **개발·운영환경 보안 취약점 점검방법을 제시**하고 있는가?

- **취약점 점검 및 조치계획의 적정성 확인**
  - **취약점 점검시기, 점검결과에 따른 조치사항, 주기적인 점검계획** 등을 포함하여 제시

* 취약점 제거 등 보안조치 수행에 있어서도, 예를 들어 취약판단을 받아도 그 위험을 최소화할 수 있는 합당한 조치와 근거를 제시할 수 있음

04 제공 역량

보안성 취약점 점검 및 조치

검토 항목

검토 내용

검토 기준

1.5 취약점 점검 및 조치(2/2)

서비스 SW 및 **개발·운영환경 보안 취약점 점검방법을 제시**하고 있는가?

* 관련서류 : 정보보호정책서, SW개발보안지침, 점검계획서 및 조치 결과보고서 등 결재 문서

* 참조문서

- 소프트웨어 보안약점 진단가이드(행정안전부, 2019.6.)
- 모바일 대민서비스 보안취약점 점검 가이드(행정자치부, 2015.12.)
- 기술적 취약점 분석평가 방법 상세가이드(과학기술정보통신부, 2017.12)
- OWASP “OWASP Top 10”, https://www.kisa.or.kr/public/laws/laws3.jsp 참조

04 제공 역량

운영안정성

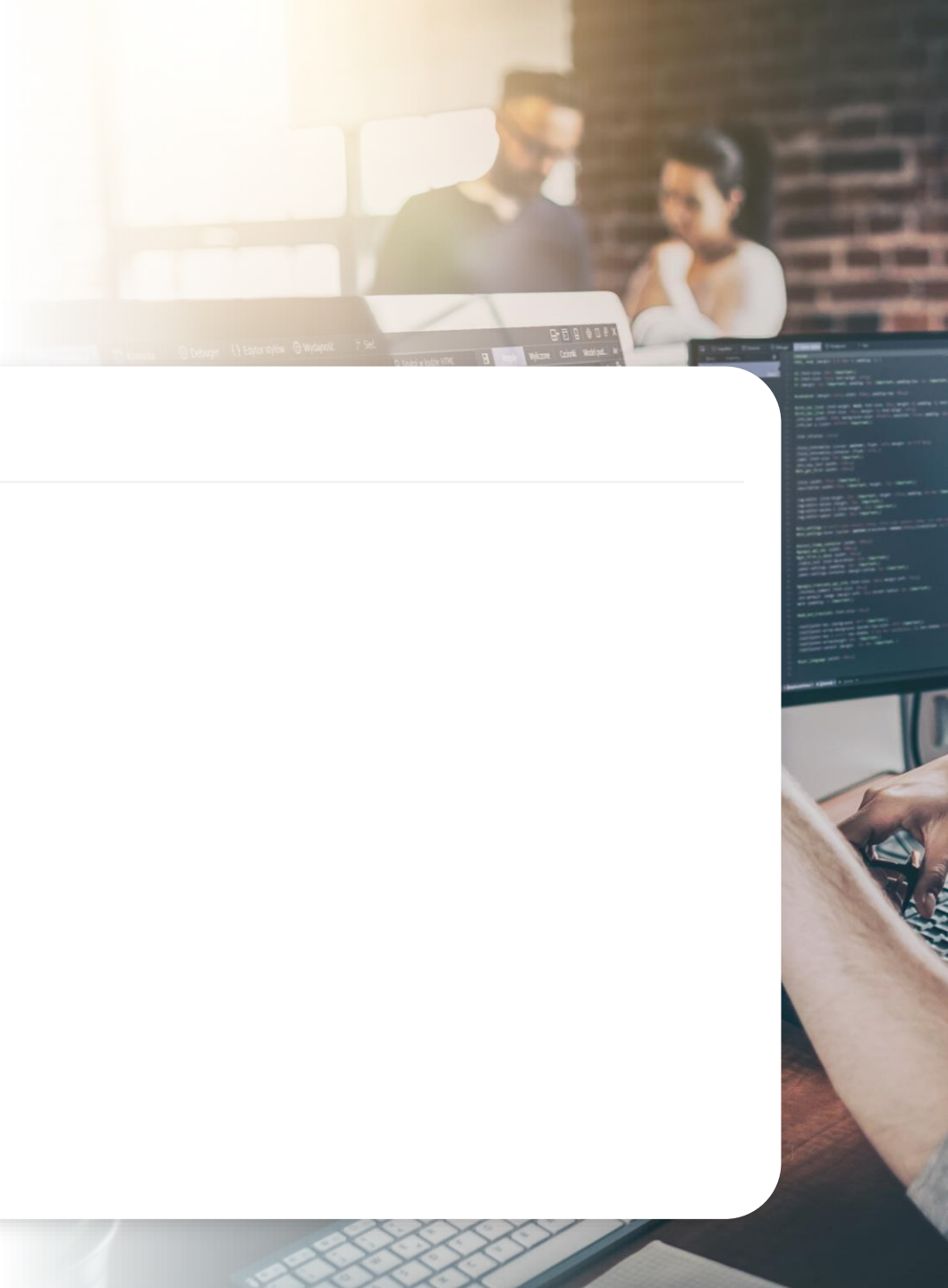
검토 항목

2. 운영안정성

2.1 가용률

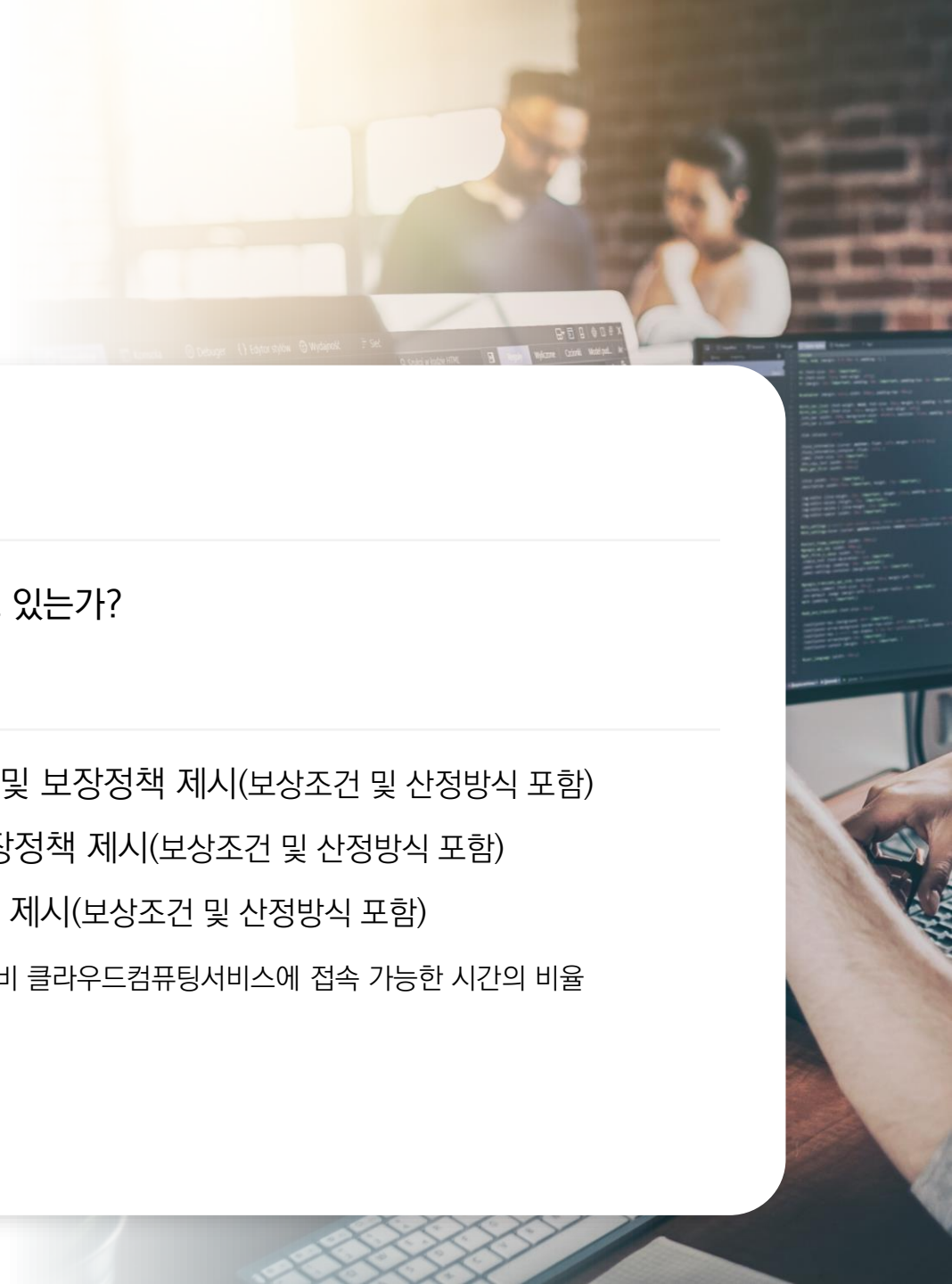
2.2 모니터링 정보

2.3 백업 및 복구



04 제공 역량

운영안정성 가용률



검토 항목

검토 내용

검토 기준

2.1 가용률(1/2)

가용률 보장정책(보상조건, 산정방식)을 제시하고 있는가?

- **IaaS, PaaS** : **99.9% 이상** 가용률 목표수준 및 보장정책 제시(보상조건 및 산정방식 포함)
- **SaaS** : **99.5% 이상** 가용률 목표수준 및 보장정책 제시(보상조건 및 산정방식 포함)
- **그 외 서비스** : 가용률 목표 수준 및 보장정책 제시(보상조건 및 산정방식 포함)

* 가용률이란 정해진 서비스 운영 시간(예정된 가동시간) 대비 클라우드컴퓨팅서비스에 접속 가능한 시간의 비율

04 제공 역량

운영안정성 가용률

검토 항목

검토 내용

검토 기준

2.1 가용률(2/2)

가용률 보장정책(보상조건, 산정방식)을 제시하고 있는가?

* 클라우드컴퓨팅서비스 품질 · 성능에 관한 기준(과학기술정보통신부, 2018.8)
* https://www.cloudqos.or.kr/page/availability 참조

04 제공 역량

운영안정성 모니터링 정보

검토 항목

검토 내용

검토 기준

2.2 모니터링 정보

리소스 모니터링 및 장애 정보를 제공하고 있는가?

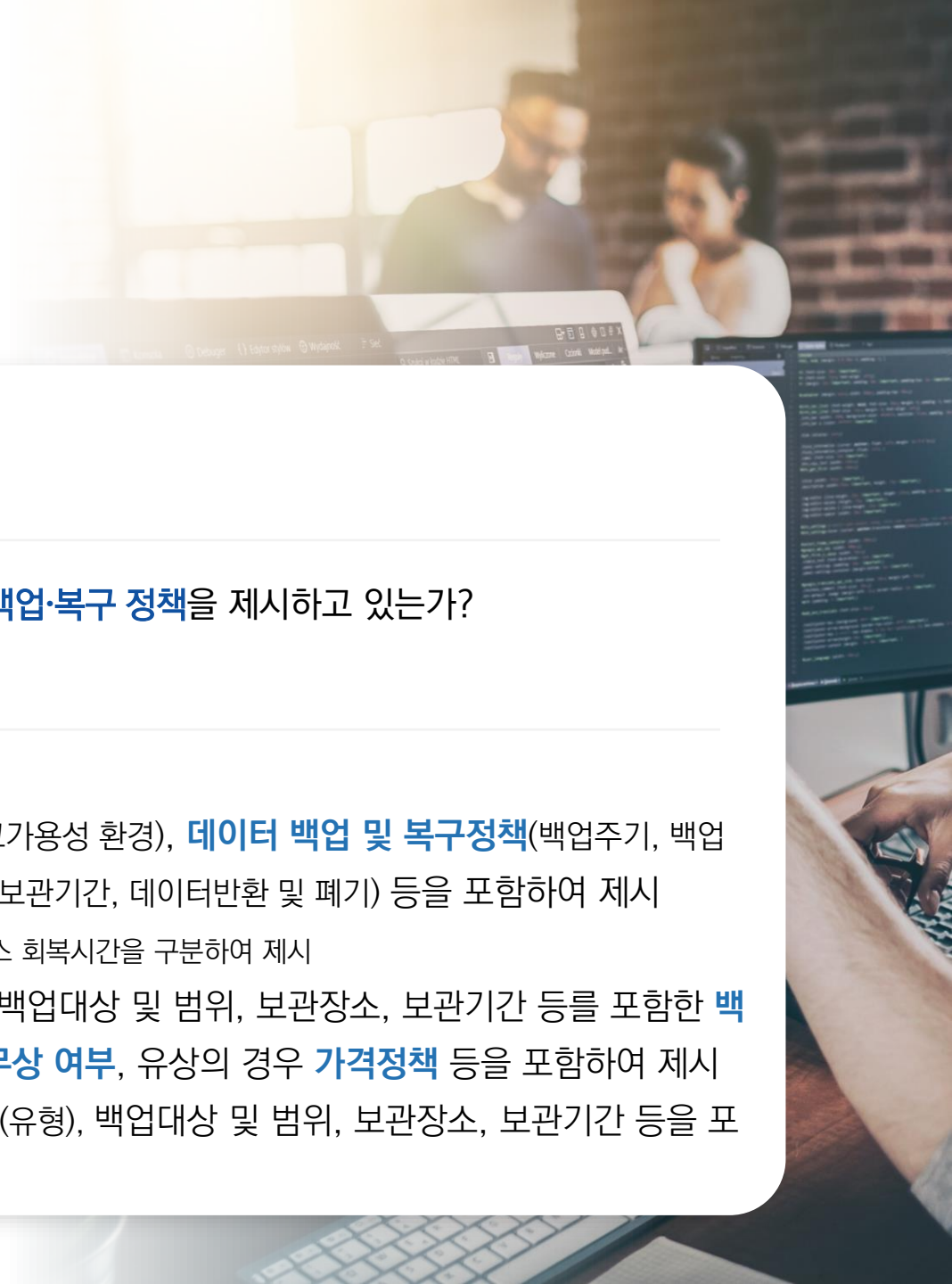
- **IaaS**: **리소스 사용량**(CPU, Memory, Disk, 트래픽 필수 포함),
  장애정보 및 장애정보 알림기능(이메일, SMS 등), **API 제공** 등을 필수 포함하여 모니터링 정보 제시
- **PaaS, SaaS**: **서비스 모니터링 제공 정보**, **제공절차**(제공주기, 제공방법) 등을 포함하여 제시
- **그 외 서비스**: 리소스 사용량, 장애정보 및 장애정보 알림기능 등 모니터링 정보제공 절차(제공주기, 제공방법) 등을 포함하여 제시

*** 이용자에게 제공 가능한 모니터링 및 장애 정보를 제시하여야 함**

* 모니터링 정보제공 절차 중 모니터링 정보의 제공주기(상시, 일/주/월 등) 및 제공방법 등 제공절차를 필수 포함하여야 함

04 제공 역량

운영안정성 백업 및 복구



검토 항목

검토 내용

검토 기준

2.3 백업 및 복구

서비스의 신속한 복구를 위한 **장애 대응체계 및 백업·복구 정책**을 제시하고 있는가?

- **장애대응체계 제시**
- **IaaS, PaaS**: **평균 서비스 회복시간**(일반 및 고가용성 환경), **데이터 백업 및 복구정책**(백업주기, 백업 준수율, 데이터복구시간 및 복구시점, 백업데이터 보관기간, 데이터반환 및 폐기) 등을 포함하여 제시
  * 일반 및 고가용성(HA, DR 등) 환경에서의 평균 서비스 회복시간을 구분하여 제시
- **SaaS** : 백업주기, 백업시간, 백업방법(유형), 백업대상 및 범위, 보관장소, 보관기간 등를 포함한 **백업정책 및 백업기능**(서비스) **제공에 따른 유·무상 여부**, 유상의 경우 **가격정책** 등을 포함하여 제시
- **그 외 서비스** : 백업주기, 백업시간, 백업방법(유형), 백업대상 및 범위, 보관장소, 보관기간 등을 포함하여 백업정책 제시

04 제공 역량

검토 항목

3. 지원 체계

3.1 조직·인력 구성 현황 및 이용자 지원

3.2 고객대응 관리체계

04 제공 역량

지원 체계 이용자 지원 체계

검토 항목

검토 내용

검토 기준

3.1 조직·인력 구성 현황 및 이용자 지원 체계

디지털 서비스의 유지 및 지원을 위한 **이용자 지원체계**를 제시하고 있는가?

- **조직인력 구성현황(디지털 서비스를 유지하기 위한 담당조직 및 역할 등)**
  - 고객 서비스 유지 및 요구사항을 원활히 지원하기 위한 **담당조직, 담당인력, 담당업무** 등 포함
- **이용자 지원체계(이용자 매뉴얼, 교육자료, 기술자료 등)**
  - 이용자 매뉴얼, 교육자료, 온라인 교육, 기술지원 등 **제공 가능한 범위의 이용자 지원 방안** 제시
- **클라우드 지원 서비스 조직 역량(* 클라우드 지원서비스 유형에만 해당되는 사항)**
  - **클라우드 지원서비스**는 클라우드 컴퓨팅서비스 도입·전환에 필요한 **업무수행(컨설팅, 운영관리, 마이그레이션 등)을 위해 관련 자격보유, 교육이수, 수행 경험 등을 포함한 조직 및 수행 인력의 역량** 제시

04 제공 역량

지원 체계 고객대응 관리체계

검토 항목

검토 내용

검토 기준

3.2 고객대응 관리체계

고객요구 접수 및 요구사항 처리를 위한 **고객대응 관리체계**를 제시하고 있는가?

- **고객의견 수렴채널(FAQ, 온라인헬프, 1:1문의, 고객센터 운영 등) 필수 제시**

– 1개 이상의 다양한 **고객의견 수렴 채널**을 제시

- **고객의견 수렴조직(담당조직, 담당자, 연락처) 및 기술지원 등 고객 피드백 절차 필수 제시**

– 고객의견 **수렴 조직 및 기술지원 조직**을 포함하여 필수 제시

* 반드시 전담조직·인력만 가능한 것은 아니나, 담당조직 및 담당자, 연락처는 필수 제시

– 고객피드백 절차 등 **내부처리 절차**를 필수 제시

* 고객요구 사항을 원활히 접수하고 처리하여 피드백하는 내부처리 및 대응절차를 필수 제시

NIA 한국지능정보사회진흥원

감사합니다