
전송자격인증제 신청서류 작성 가이드라인

- 신청기업용 -

2026. 7.



방송미디어통신위원회

Korea Media and Communications Commission

제·개정이력

순번	제·개정일	변경내용	발간부서	연락처
1	2026.4	제정	디지털이용자기반과	-
2	2026.6	개정	디지털이용자기반과	-
3	2026.7	개정	디지털이용자기반과	-
4	2026.10	개정	디지털이용자기반과	-

목 차

1. 개 요	1
2. 전송자격의 인증 기준 해설	4
2.1. 서류의 적정성	4
2.2. 이용자 관리의 적정성	8
2.3. 보안체계의 적정성	11
2.4. 기록 관리의 적정성	16
2.5. 조치의 적정성	18
3. 증빙자료	20

1. 개 요

문자 발송 서비스를 제공하고자 하는 자는 「전기통신사업법」 제22조의11(전송자격인증)에 따라 불법스팸 전송 방지를 위한 전송자격인증 기준을 충족하여야 합니다.

전송자격인증제는 문자발송 시스템이 불법스팸 전송의 매개가 되지 않도록 하기 위한 제도로, 불법스팸의 유통을 사전에 차단하고 이용자 보호를 강화하기 위해 「불법스팸 방지 종합대책」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「개인정보 보호법」 등에 근거하여 정보통신서비스 제공자가 준수해야 할 기술적·관리적·운영상 조치 기준으로 구성되어 있습니다.

본 문서는 전송자격인증 기준의 내용을 정보통신서비스 제공자의 입장에서 쉽게 이해할 수 있도록 설명하고, 수검 시 필요한 구체적인 점검항목, 준비사항, 증빙자료 예시를 제시함으로써 인증 준비를 원활하게 지원하고자 마련했습니다.

전송자격인증기준은 보안체계, 로그관리, 이용자 관리, 불법스팸 대응 조치 등의 적정성을 확인함으로써 문자발송 시스템에 대한 해킹 등 외부로부터 공격을 예방하고, 내부자의 부적정한 이용을 방지하며, 불법스팸을 발송한 스팸머의 확인·추적의 용이성을 확보하는 등 정보통신서비스 제공자로서 최소한의 적격 여부를 확인하는 데 그 목적이 있습니다.

이에 따라, 정보통신서비스 제공자는 전송자격인증 기준에 따른 인증 항목 및 인증 절차에 대해 적절한 조치를 취하고, 인증 과정에서 요구되는 서류, 시스템, 정책 등을 체계적으로 준비해야 합니다.

각 사업자는 안전하고 책임성 있는 문자 발송 서비스를 구축함으로써 전송자격인증을 준비하는 과정에서 본 가이드라인을 활용할 것을 권고합니다.

〈 전송자격인증 기준 (방송미디어통신위원회 고시 제2026-1호) 〉

분야		항목		상세 기준
1.	서류 적정성	1.1.	이용약관	서비스 이용약관 및 계약서에는 불법스팸 관련 책임을 명시하고, 이를 통해 이용자가 불법스팸 전송에 대한 법적 책임과 서비스 이용 제한 가능성을 쉽게 인식할 수 있도록 하여야 한다.
		1.2.	사무실 확보증명서	소유권·임차권 등을 확인할 수 있는 서류가 적정하여야 한다.
		1.3.	불법스팸 발송 방지계획서	불법스팸 방지를 위한 문자발송 시스템 운영, 불법스팸 발송자에 대한 계약해지, 발송정지 등 불법스팸 방지계획서가 적정하여야 한다.
2.	이용자 관리의 적정성	2.1.	계정관리	이용자 계정은 무단으로 사용되지 않도록 다음과 같이 제한한다. 가. 이용자 1인당 계정은 1개 나. 계정당 등록 가능한 무선발신번호는 개인인 경우에는 3회선(외국인은 2회선), 법인인 경우에는 4회선 다. 계정당 등록 가능한 유선발신번호(인터넷전화 등)는 개인인 경우에는 5회선, 법인인 경우에는 종사자 수
		2.2.	국외 이용자	국외 IP는 문자발송 시스템 접근을 차단한다. 다만, 해외거주자, 해외법인 등의 경우에는 필요서류를 받아 관리자 확인 후 허용한다.
		2.3.	부정사용 차단	발신번호의 명의자(이용자)와 이용료 납부자의 일치 여부를 확인하여 부정사용을 차단하여야 한다.
3.	보안체계의 적정성	3.1.	방화벽 설치	문자발송 시스템에 외부 침입을 방지하기 위한 방화벽을 구축하여야 한다.
		3.2.	접근권한 부여의 적정성	문자발송 시스템 접근권한이 없는 자의 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여하는 관리체계를 마련하여야 한다.
		3.3.	접근권한 변경의 적정성	전보 또는 퇴직 등 인사이동 발생 시 지체 없이 문자전송 시스템 접근권한을 변경 또는 말소하여야 한다.
		3.4.	다중 인증	이용자의 계정이 제3자에 의해 무단으로 사용되지 않도록 다중 인증 방식을 적용하고, 로그인 실패 횟수 제한과 불법 로그인 시도 시 경고기능 등 비인가자의 문자발송 시스템 접근을 차단하기 위한 기술적·관리적 조치 계획을 수립하고 이행하여야 한다.
		3.5.	추가 인증	문자 발송 시 해당 발신번호에 대해 추가적인 본인인증 절차를 수행하여 발송 계정의 정당성을 확인하여야 한다.

분야		항목		상세 기준
4.	기록 관리의 적정성	4.1.	이용자 로그 관리	이용자 접속기록, 인증기록, 문자발송 이력, 과금이력 로그는 관련 법령에서 정한 최소 보관 기간 이상(법령에서 정하는 기간이 별도로 없는 경우 1년) 보관하여야 한다.
		4.2.	시스템 로그 관리	문자발송 시스템 접속기록, 문자발송 시스템 오류 및 장애 로그, 개인정보 조회·수정·삭제 이력 관련 로그는 관련 법령에서 정한 최소 보관 기간 이상(법령에서 정하는 기간이 별도로 없는 경우 1년) 보관하여야 한다.
		4.3.	로그 점검	이용자 로그 및 문자발송 시스템 로그는 주기적으로(월1회) 점검하고 그 결과를 보관·관리하여야 한다.
5.	조치 적정성	5.1.	조치 및 결과확인	불법스팸 신고내역을 모니터링한 결과 또는 정부에서 제공하는 정보를 통하여 불법스팸 전송 사실을 확인한 경우 해당 이용자 또는 관련 발신번호에 대한 서비스 제공을 중단하는 등의 조치를 하고 그 결과를 확인·보관하여야 한다.
		5.2.	금칙어 등 차단 체계 운영	불법스팸방지를 위한 금칙어, 악성 URL 차단 체계를 운영하고, 차단결과를 관련 법령에서 정한 최소 보관 기간 이상(법령에서 정하는 기간이 별도로 없는 경우 1년) 보관하여야 한다.

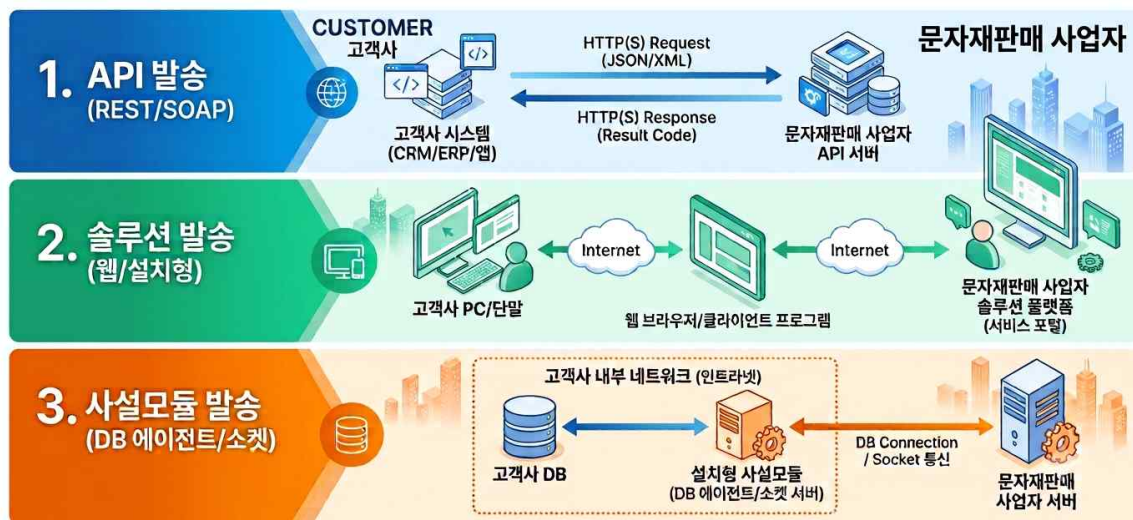
※ 방송미디어통신위원회는 전송자격인증신청자(대표자 등)가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제50조부터 제50조의8을 위반하여 제재받은 사실과 한국인터넷진흥원에 신고된 불법스팸 건수를 확인하고 이를 심사에 참고할 수 있다.

2. 전송자격인증 기준 심사항목 별 해설

< 용어 정의 >

용어	정의
이용자	문자발송 사업자가 제공하는 서비스를 이용하는 모든 이용자 ※ 문자발송 웹페이지를 이용하는 개인·법인(B2C) 및 계약관계에 있는 문자발송 사업자(B2B)를 포괄
발송 계정	문자발송 시스템에 접속하여 발신번호 등록, 문자 발송, 발송 이력 조회 등 발송 관련 기능을 수행하는 이용자 계정. 기업회원의 경우 실제 발송자인 임직원 계정을 포함
웹페이지 발송	이용자가 웹 브라우저를 통해 문자발송 서비스 화면에 접속하여 직접 문자 발송을 요청하는 방식
API·솔루션·모듈 발송	고객사 시스템, 외부 프로그램, 연동 모듈, 자동화 서버 등을 통해 문자 발송이 이루어지는 방식
다중인증	계정 접속 시 ID/PW 외에 회원가입 시 본인확인 및 등록 확인된 정보를 기반으로 계정 소유자 또는 정당 이용자 여부를 추가 확인하는 절차
추가인증	문자 발송 시 등록 발신번호와 발송 계정의 정당한 연계성을 확인하기 위해 수행하는 발신번호 기반 인증 또는 계정·서비스 연계 확인 절차
시스템적 통제	기준 충족 여부를 담당자의 임의 판단이나 수기 대장에만 의존하지 않고, 시스템 기능으로 차단·보류·승인·기록·조회할 수 있도록 구현하는 것을 의미

사업자 발송 유형



※ AI로 생성된 이미지입니다.

2.0. 전송자격인증제 신청

- 서비스 유형 별(웹페이지, API, 솔루션, 모듈 등) 인증기준에 맞는 증빙자료를 제출해야 합니다.
※ 웹페이지 발송과 API 발송을 모두 제공하는 경우 각 발송 유형 별 증빙자료를 제출해야 하며, 증빙자료가 동일한 경우 이전 제출자료로 갈음할 수 있습니다.
- 별도의 신청서류 양식은 제공되지 않으며 사업자 자체 양식으로 작성하여 제출하시면 됩니다.
- 전송자격인증제 서류 심사는 인증기준 준수 여부를 확인할 수 있는 화면 캡처, 문서 양식, 실제 관리 문서 사진, 설명자료 등 제출서류를 기준으로 진행됩니다. 제출서류를 통해 인증기준 적용 여부를 확인하기 어려운 경우 서류에 대한 보완 또는 인증기준 부적합으로 판단될 수 있습니다.
- 전송자격인증제 현장 심사는 인증기준에 부합하는 시스템을 구축하였는지 확인하며, 제출서류와 상이하거나 시스템적 통제 기능 도입이 미비한 경우 보완 또는 부적합으로 판단될 수 있습니다.

2.1. 서류 적정성

항목	1.1. 이용약관
상세 내용	▶ 사업자는 자사가 제공하는 문자발송 서비스 전반에 대한 이용약관, 계약서 또는 운영정책을 마련해야 한다. ▶ 이용약관 또는 계약서에는 불법스팸 전송 금지 조항, 위반 시 서비스 정지·해지, 발송 제한, 법적 책임 및 역무제공거부가 명시되어야 한다. ▶ 웹페이지 발송, API·솔루션·모듈 제공, 기업 간 계약 등 서비스 유형별로 이용자에게 적용되는 약관 또는 계약 조건이 확인되어야 한다.
주요 확인 사항	① 문자발송 서비스와 관련한 모든 이용약관, 계약서 또는 운영정책이 제출되었는가? ② 불법스팸 전송 금지 및 정보통신망법상 의무 준수 조항이 포함되어 있는가? ③ 위반 시 서비스 정지·해지, 발송 제한, 손해배상 또는 법적 책임 가능성이 명확히 고지되어 있는가? ④ 회원가입, 계약 체결 또는 서비스 신청 단계에서 이용자가 해당 내용을 확인하고 동의했는가? ⇒ 불법스팸 전송금지와 역무제공거부 근거를 명확히 고지하고, 이용자 동의 절차를 투명하게 운영
항목 해설	【설 명】 • 웹페이지 문자 발송 서비스는 회원가입 단계에서 이용약관을 고지하고 이용자의 동의 후 서비스를 제공해야 합니다. • 기업 간 계약 방식은 별도 웹페이지 약관이 없더라도 계약서, 서비스 신청서, 운영정책 등에 불법스팸 금지 및 제재 조항을 포함해야 합니다. • 불법스팸 전송 금지 및 역무제공거부 조항은 실제 조치 기준과 연계되어야 하며, 5.1 조치 및 결과확인 항목의 서비스 거부, 이용계약 해지 등의 근거로 활용될 수 있어야 합니다. • 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제50조, 제50조의8의 불법스팸 전송 금지 조항이 포함되어야 합니다. • 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(26.10.1. 시행) 제50조의4에서 규정한 정보통신서비스 제공자의 조치의무를 이행할 수 있도록 반영해야 합니다. 【주의사항】 • 약관은 실제 서비스 유형별로 적용 가능해야 하며, 형식상 조항만 존재하고 이용자에게 고지되지 않은 경우 보완이 필요할 수 있습니다. • 약관에 전송자격인증제의 인증주체 등을 반영한 경우, 그 인증주체를 “방송미디어통신위원회”로 규정해야 합니다. 【증빙자료】 • 이용약관 전문 • (있는 경우) 기업 간 계약서 또는 서비스 신청서 • 불법스팸 및 역무제공거부 조항 발췌 • (웹페이지 발송) 회원가입 시 약관 동의 화면 캡처

항목	1.2. 사무실 확보증명서
상세 내용	▶ 사업자는 신뢰성과 실체성을 확보하기 위해 사무공간을 확보해야 한다. ▶ 신청서 상의 주소와 제출 서류의 주소가 일치하고, 실제 입주 또는 사용 여부가 확인되어야 한다.
주요 확인 사항	① 신청서와 임대차계약서, 이용계약서, 등기부등본 등의 주소가 일치하는가? ② 공유오피스·자택 사업장인 경우 실제 이용계약 및 실사용 증빙이 있는가? ③ 현장 점검 또는 통지 수령이 가능한 실제 사업장인지 확인되는가? ⇒ 실제 사업장 확보 여부 및 현장 점검 장소 확인
항목 해설	【설 명】 - 공유오피스는 이용계약서와 입주확인서 등 실제 사용 사실을 확인할 수 있는 자료를 제출합니다. - 자택 사업장은 사업자등록 주소, 등기부등본, 공과금 내역 등 실사용 여부를 확인할 수 있는 자료를 준비합니다. 【주의사항】 - 단순 주소 기재만으로는 실제 확인이 어려우므로 실제 업무 공간이라는 점을 입증해야 합니다. 【증빙자료】 - 임대차계약서 - 등기부등본 - 기타 사업자등록증 상 주소지 확인자료 - 공유오피스 이용계약서·입주확인서 (실사용 증빙이 필요한 경우) 공과금 내역

항목	1.3. 불법스팸 발송 방지계획서
상세 내용	▶ 사업자는 불법스팸 유통을 방지하기 위한 예방·탐지·조치·재발방지 체계를 갖추고 이를 문서화한 「불법스팸 발송 방지계획서」를 제출해야 한다. ▶ 계획서는 선언적 문구가 아니라 실제 운영 프로세스, 책임자, 시스템 통제, 모니터링, 제재 및 교육계획을 포함해야 한다. ▶ 양식 내 회색 안내 문구는 작성 예시이므로 그대로 제출할 필요는 없으나, 안내 항목은 자사 운영 방식에 맞게 구체화해야 한다.
주요 확인 사항	① 전담조직, 책임자, 담당 인원 및 운영계획이 포함되어 있는가? ② 회원가입, 발신번호 등록, 입금자 확인, 스팸 신고내역 확인, 이용제한, 하위사업자 제재 등 업무별 절차가 구체적인가? ③ 이상징후 모니터링 및 재발방지 절차가 마련되어 있는가? ④ 임직원 교육계획 및 점검주기가 포함되어 있는가? ⇒ 불법스팸 방지를 위한 체계적이고 구체적인 계획을 보유하고 있는지 확인
항목 해설	【설 명】 • 계획서에는 불법스팸 신고내역 확인 주기, 조치 기준, 통보 방법, 조치 결과 보관 방법을 포함합니다. • 이상징후 모니터링은 야간 발송, 발송량 급증, 신규 계정의 단기간 대량 발송, 동일 문구·URL 반복 발송 등을 기준으로 설정할 수 있습니다. • 양식의 회색 문구는 작성 가이드이므로 삭제할 수 있으나, 해당 항목이 미적용되는 경우에는 “해당 없음”과 그 사유 또는 대체 운영 방식을 기재하는 것이 적절합니다. 【주의사항】 • 계획서의 내용은 실제 운영 절차와 일치해야 하며, 심사 시 이행 여부가 확인될 수 있습니다. 【증빙자료】 • 불법스팸 발송 방지계획서 ※ 가이드라인에 포함된 양식은 샘플자료이며, 사업자 자율 양식으로 제출 가능

2.2. 이용자 관리의 적정성

항목	2.1. 계정관리
상세 내용	▶ 이용자 계정은 불법스팸어의 재발송 방지, 신속한 차단 및 발송자 추적을 위한 핵심 요소이다. ▶ 회원가입 시 검증된 본인확인기관의 서비스를 통해 이용자 본인확인을 수행하고, 본인확인 결과를 계정과 연계하여 중복가입을 차단하여야 한다. ▶ 계정 및 발신번호 제한 기준은 담당자 수기 관리가 아니라 시스템적으로 통제되어야 한다. ▶ 1인 1계정 원칙은 기업 1개당 1계정이라는 의미가 아니라 실제 문자발송 시스템을 이용하는 발송자 1인당 1계정 사용을 원칙으로 한다.
주요 확인 사항	①-1 (웹페이지 발송) 계정 생성 시 검증된 본인확인기관 서비스 등을 통해 본인확인을 수행하고 있는가? ①-2 (사설발송) 계정 발급 시 계약 등을 통해 이용자의 본인확인을 수행하고 있는가? ② 계정 생성 시 중복가입을 시스템적으로 차단하고 있는가? ③ 발신번호 등록 시 개인·외국인·법인 등 이용자 유형별 회선 수 제한이 시스템적으로 적용되는가? ④ 회선 수를 초과하여 등록할 수 없도록 시스템적으로 통제되는가? ⑤ 기업 간 계약의 경우 사업자 확인, 통신서비스 이용증명원, 재직증명서 등 증빙자료를 확인하고 발송 계정(이용자)별로 발신번호를 분류하고 있는가? ⇒ 1인 1계정, 발신번호 수 제한, 증빙자료 확인, 등록·변경·삭제 이력을 시스템적으로 통제해야 한다.
항목 해설	【설 명】 • 회원가입 단계에서는 검증된 본인확인기관 서비스를 통해 이용자를 확인하는 것을 원칙으로 합니다. • 계약관계를 통한 계정 발급 시 신원을 확인해야 하며, 중복 가입을 통제하는 절차를 마련해야 합니다. • 소셜계정 연동 회원가입은 가입 편의 수단으로 활용할 수 있으나, 이메일·닉네임·프로필 정보만으로 본인확인 및 중복가입 차단 요건을 충족한 것으로 보기 어렵습니다. • 기업회원의 경우 실제 발송자별 계정을 발급하고, 부서·지점·업무별 권한과 사용 가능한 발신번호, 발송 이력이 구분되어야 합니다. • 공용 계정 사용, 발송자 식별이 어려운 계정 운영, 발신번호와 실제 이용자 간 연계가 불명확한 방식은 운영이 불가합니다. • 무선 발신번호는 이용자 본인 명의 여부를 확인하고, 유선 발신번호는 통신서비스 이용증명원, 재직증명서, 위임장, 위수탁계약서 등으로 사용권한을 확인합니다. • 법인 대표번호 또는 공동 사용번호는 최초 등록 시 통신서비스 이용증명원과 사업자등록증으로 소유·가입관계를 확인하고, 이후 직원 추가 시에는 기존 증빙자료를 시스템에 연계하여 재사용할 수 있습니다. 이 경우 추가 직원별 재직증명서와 발신번호 사용권한 신청서 또는 중복등록신청서를 관리해야 합니다. • 무선 발신번호의 경우 최대 회선 수를 개인 3회선(외국인 2회선), 법인 4회선으로 제한합니다. • 유선 발신번호의 경우 최대 개인 5회선, 법인 n회선(n = 종사자 수)으로 제한합니다. ※ 기업의 고용보험 자료나 종사자 수를 확인할 수 있는 자료를 제출받아 적용할 수 있습니다. 【주의사항】 • 단순 수기 대장만으로 계정 및 발신번호 제한 기준을 관리하는 방식은 인증기준에 부적합합니다. • 수기 확인은 통신서비스 이용증명원 진위 확인, 재직증명서 확인, 위임장 검토 등 보완 절차로 활용할 수 있으나, 최종 등록 가능 여부 판단, 초과등록 보류·승인, 이력관리는 시스템에서 이루어져야 합니다. • 기존 등록 발신번호도 심사 및 사후점검 과정에서 관리 대상이 될 수 있으므로 발신번호별 증빙자료를 정비해야 합니다. 【증빙자료】 • 회원가입 과정 중 본인확인 및 중복가입 차단 화면 • 계정별 발신번호 초과 등록 제한 화면 • 발신번호 등록·변경·삭제 이력

항목	2.2. 국외 이용자
상세 내용	▶ 국외 IP 또는 VPN·프록시 등 우회접속을 활용한 문자발송 시스템 악용을 방지하기 위해 국외 IP 접근 차단 및 우회접속 방지체계를 운영해야 한다. ▶ 지정 IP만 허용하는 화이트리스트 방식이 모든 접근 경로에 적용되고 미등록 IP가 차단되는 경우 국외 IP 차단 및 우회접속 방지 대책의 하나로 인정될 수 있다.
주요 확인 사항	① 국외 IP 주소에 대한 차단 정책이 시스템에 적용되어 있는가? ② 해외거주자, 해외법인, 국외 출장자 등 예외 이용자 허용을 위한 증빙자료와 관리자 승인 절차가 있는가? ③ (운영시) 허용 IP 등록·변경·삭제 이력, 허용 기간, 승인자, 승인 사유가 시스템에 기록되는가? ④ VPN, 프록시, Tor, 클라우드 익명 접속 등 우회접속 위험을 탐지·차단하거나 합리적으로 통제하는 절차가 있는가? ⑤ 문자발송 페이지, 관리자 페이지, API, 모듈 연동 서버 등 모든 접근 경로가 통제 대상에 포함되는가? ⇒ 국외 IP의 접근 차단 및 우회접속 방지체계를 시스템적으로 운영하고 예외 허용 이력 보관
항목 해설	【설 명】 • 국가코드 기반 차단, 국내 IP 대역 허용, 지정 IP 화이트리스트, VPN·프록시 탐지 서비스, 접속지 불일치 탐지 등 서비스 특성과 위험도에 맞는 방법을 사용할 수 있습니다. • 지정 IP 허용 방식은 등록되지 않은 IP를 국내·국외 여부와 관계없이 차단하는 구조라면 별도의 국가코드 기반 차단 솔루션을 중복 구축하지 않더라도 국외 IP 차단 목적을 상당 부분 충족할 수 있습니다. • 다만 허용 IP가 국외 IP, VPN, 프록시, 클라우드 익명 접속 대역에 해당하지 않는지 확인하고, 허용 IP 등록·변경·삭제 절차를 관리자 승인 기반으로 운영해야 합니다. 【주의사항】 • VPN·프록시를 100% 탐지하는 것은 현실적으로 어려울 수 있으나, 어떤 탐지·차단·승인 등 통제 절차가 없는 경우 보완이 필요합니다. • 관리자 페이지에는 IP 제한이 있으나 발송 API에는 제한이 없는 등 일부 접근 경로가 누락되지 않도록 확인해야 합니다. 【증빙자료】 • 국외 이용자 및 우회접속 방지체계 적용 증빙자료 - 네트워크 차단 정책(설정 화면 등 캡처) - 등록된 IP 접근 허용 정책(설정 화면 등 캡처) - 접근제어 정책(국외 IP 차단 설정 화면 캡처) - 접근제어 정책(예외 이용자 허용 설정 화면 캡처) - 관리자 수동 승인 절차(화면 캡처) 등 • 우회 접속 방지를 위한 기술적 조치 사항 • 우회 접속 방지를 위한 기술적 조치 설명자료

항목	2.3. 부정사용 차단
상세 내용	▶ 사업자는 서비스 이용료 납부 내역, 실제 서비스 이용자, 발신번호 명의자 또는 사용권한자가 계정 기준으로 식별·연계되도록 관리하여 부정사용을 차단해야 한다. ▶ 계정 명의자 외 명의 결제, PG 결제 명의 확인 곤란, 기업 내부 정산, 가상계좌 자동매칭 등 다양한 결제 구조를 고려하되, 사후 추적과 소명·보류·제한 절차가 시스템적으로 운영되어야 한다.
주요 확인 사항	① 자동이체, 가상계좌, 카드결제, 휴대폰 결제, 무통장입금 등 결제정보가 계정과 명확히 연결되는가? ② 명의 불일치, 제3자 결제, 이상거래 등 의심 건에 대해 보류·소명·환불 서비스 제한 등 절차가 운영되는가? ③ 처리 결과가 계정별로 기록·보관되는가? ⇒ 결제정보, 계정정보, 발신번호 정보를 사후 추적 가능하게 연계하여 비정상 거래 차단
항목 해설	【설 명】 - PG 결제 특성상 결제 명의자 정보를 직접 제공받지 못하는 경우에는 주문번호, 승인번호, 결제금액, 결제일시, 결제수단 등을 이용자 계정별로 기록·관리합니다. - 가상계좌 1:1 매칭, 주문번호 기반 자동 식별, 고유 식별코드 부여 등으로 입금 내역이 특정 이용자 계정에 정확히 귀속되고 사후 확인이 가능하다면 자동화 시스템을 운영할 수 있습니다. - 기업회원의 대표자 또는 임직원 명의 결제는 법인계약, 내부 정산, 위임관계 등 정당한 결제 관계가 확인되고 결제정보와 이용자 계정 간 연계되는 경우 운영할 수 있습니다. - 동일인 또는 정당한 결제 관계가 확인되지 않은 입금 건은 즉시 충전하지 않고 보류한 뒤, 소명자료 확인 후 처리해야 합니다. 【주의사항】 “입금자명=이용자명=발신번호 명의자”를 항상 실시간으로 1:1 강제 대조해야 한다는 의미는 아니지만 부정사용 의심 사례를 탐지·보류·소명·제한할 수 있는 체계가 필요합니다. - 동일인이 아니거나 정당한 관계가 확인되지 않았을 때 해당 결제 건에 대한 서비스 제공을 제한하고 필요한 조치를 해야 합니다. 【증빙자료】 - 이용료 납부 내역 관리대장 ※ 전자문서(엑셀파일 등) 또는 수기 관리하는 경우 내용이 없어도 사진 또는 캡처하여 제출 - 서비스 제공 거부 처리조치(있는 경우) - 부정사용 차단 관련 모든 처리 결과(있는 경우) ※ 이용자 별 이용료 납부 내역, 처리 결과 등

2.3. 보안체계의 적정성

항목	3.1. 방화벽 설치
상세 내용	▶ 방화벽은 문자발송 시스템 및 관련 주요 설비의 침해사고 예방과 대응을 위한 1차 보호장치이다. ▶ 전용 물리장비뿐 아니라 클라우드 보안기능, 가상 방화벽, 범용 서버 기반 네트워크 방화벽 등도 실제 네트워크 경계에서 접근통제 정책을 적용하고 로그·모니터링 체계를 갖춘 경우 검토될 수 있다.
주요 확인 사항	① 문자발송 시스템 및 관련 주요 설비가 방화벽 또는 이에 준하는 네트워크 접근통제 체계를 통해 보호되고 있는가? ② 허용·차단 정책이 업무 목적에 맞게 설정되어 있는가? ③ 관리 편의성을 위한 우회 접속 또는 비가시성 경로가 없는가? ④ 방화벽 정책 변경 및 관리자 접근 이력이 관리되는가? ⇒ 네트워크 경계 방화벽 또는 이에 준하는 접근통제 체계 운영
항목 해설	【설 명】 - 주요 설비에는 문자발송 서버, DB 서버, 인증 시스템, 관리자 시스템, API 서버, 스토리지, 네트워크 장비 등이 포함될 수 있습니다. - 클라우드 또는 호스팅 환경에서는 클라우드 보안 기능, 네트워크 ACL, WAF, 가상 방화벽 등의 정책 정보를 증빙자료로 제출할 수 있습니다. - 단말 OS 방화벽만으로 주요 설비 전체 보호를 대체하기는 어렵습니다. 【증빙자료】 - 방화벽 장비 또는 서비스 정보 - 방화벽 동작(구동) 및 정책 화면 - 특부가 서비스와 관련된 모든 설비를 포함한 네트워크 구성도

항목	3.2. 접근권한 부여의 적정성
상세 내용	▶ 문자발송 시스템 접근권한은 업무 목적에 따라 최소 권한으로 부여되어야 한다. ▶ 관리자, 운영자, 보안담당자, 고객지원 담당자 등 역할별 권한을 구분하고 실제 시스템 권한과 권한관리대장이 일치해야 한다.
주요 확인 사항	① 관리자 및 직원별 접근권한 대장을 작성하고 있는가? ② 시스템상 계정 권한과 문서상 권한이 일치하는가? ③ 권한 부여 시 승인자, 부여 사유, 부여 일시가 기록되는가? ④ 계정 공유 또는 공용 관리자 계정 사용을 제한하고 있는가? ⑤ 사업자의 관리 및 통제 권한을 벗어난 계정이 있는가? ⇒ 접근권한은 최소권한, 업무분리, 권한검증, 최소접근 원칙에 따라 관리한다.
항목 해설	【설 명】 • 신규 계정 생성 시 담당자, 권한, 승인자, 부여 사유 등을 확인할 수 있으면 전자결재, 권한신청서, 관리자 콘솔 승인 이력 등으로 대체할 수 있습니다. • 솔루션 등 사설발송 모듈에 접근이 불가능한 경우 별도 접근권한 증빙이 불필요할 수 있으나, 원격 유지관리 계정이 있는 경우 해당 계정에 대한 증빙이 필요합니다. 【주의사항】 • 관리자 권한은 일반 발송 권한보다 위험도가 높으므로 더 엄격한 다중인증 및 권한점검이 필요합니다. • 클라우드 또는 호스팅서버를 이용하는 경우 사업자의 시스템은 타 사업자의 설비와 물리적 또는 논리적으로 분리되어 있어야 하며, 통제 범위를 벗어난 접근경로가 없어야 합니다. 【증빙자료】 • 계정 목록 및 권한분류표(계정ID, 소속, 권한 수준 명시) ※ 권한 수준의 경우 읽기(Read), 쓰기(Write), 삭제>Delete) 중 가능한 모든 권한을 작성 • 관리자 권한 설정 화면 캡처(일부 설정만 가능하도록 제한된 UI 화면 등) • 조직도(시스템 접근권한이 부여된 부서만)

항목	3.3. 접근권한 변경의 적정성
상세 내용	▶ 전보, 휴직, 퇴사 등 인사이동 시점에 해당 인력의 시스템 접근권한을 지체 없이 변경 또는 말소해야 한다. ▶ 권한 변경 내용은 시스템 로그와 관리대장으로 기록·관리되어야 한다.
주요 확인 사항	① 인사이동 또는 퇴사 발생 시 접근권한을 지체 없이 변경·삭제하고 있는가? ② 권한 변경·삭제 일시, 대상 계정, 사유, 승인자, 처리자가 기록되는가? ③ 정기적으로 현행 권한 목록과 실제 재직·업무상 필요 여부를 점검하는가? ⇒ 퇴사자 및 인사이동 계정은 지체 없이 파기 또는 변경하고 이력 관리
항목 해설	【설 명】 • 퇴사자가 퇴사 후에도 시스템에 로그인할 수 있는 상태는 불법스팸 발송 및 개인정보 유출 위험으로 이어질 수 있습니다. • 권한 변경 기준은 내부 정책으로 정하고, 인사발령·퇴직 자료와 권한 변경 이력을 연계해 보관합니다. 【주의사항】 • 권한 회수 지연 사례가 반복될 경우 접근권한 관리체계 전반에 대한 보완이 필요할 수 있습니다. 【증빙자료】 • 접근권한 변경 이력 및 사유 관리대장 ※ 전자문서(엑셀파일 등) 또는 수기 관리하는 경우 내용이 없어도 사진 또는 캡처하여 제출 • 현재 시스템 접근권한 부여 리스트(계정별 권한 조회 화면 캡처) • 계정 생성/삭제 로그(특정 계정의 생성, 수정, 삭제 기록) • 접근권한 변경 이력 자료와 관련된 근거 증빙자료 제출 ※ 인사이동, 퇴사 등에 관한 자료

항목	3.4. 다중 인증
상세 내용	▶ 단순 ID/PW만으로는 계정 탈취 위험이 크므로, 이용자 계정 접속 시 다중인증 방식을 적용해야 한다. ▶ 회원가입 시 확인·등록된 정보를 기반으로 신뢰할 수 있는 다중인증 수단을 도입할 수 있다. ▶ 비인가 접근 시도에 대해서는 로그인 실패 횟수 제한, 계정 잠금, 경고 안내 등 기술적·관리적 조치를 운영해야 한다. ▶ 사설발송 구조의 경우에도 비인가 접근, 계정 탈취, 연동정보 도용 등을 방지하기 위한 인증 및 접근통제 수단을 마련하여야 한다.
주요 확인 사항	① 계정 로그인 시 ID/PW 외에 추가 인증수단(MFA)이 도입되어 있는가? ② 다중인증 수단이 본인확인 또는 회원가입 시 등록·확인된 정보와 연계되어 있는가? ③ 인증수단 등록·변경·재설정 과정에서 재확인 및 이력관리가 이루어지는가? ④ 로그인 실패 횟수 초과 시 계정 잠금 및 경고 안내가 이루어지는가? ⑤ 소셜계정 로그인만으로 문자발송 시스템 접근을 허용하지 않고 별도 다중인증을 운영하는가? ⑥ (3.4. 다중 인증, 3.5. 추가 인증) 사설발송 유형별 Agent, API Key, 인증서 등 발송 요청 인증수단이 관리되고 있는가? ※ Agent 고유 식별값 관리, API Key 관리, mTLS 등 서버 인증 등 ⇒ 계정 탈취 및 비인가 접근을 방지하기 위한 다중인증 및 로그인 차단 기능 운영
항목 해설	【설 명】 • 다중인증 수단으로 계정에 등록·확인된 정보(휴대폰번호, 이메일 등) 기반 SMS OTP, 이메일 OTP, 앱 푸시 인증, 인증앱 OTP 등도 계정 소유자 확인을 위한 다중인증 수단으로 사용할 수 있습니다. • SMS·이메일·인증앱 OTP는 회원가입 단계의 본인확인을 대체하는 수단이 아니며, 본인확인된 계정에 등록·확인된 정보를 기반으로 안전하게 운영되는 경우 다중인증 수단으로 활용할 수 있습니다. ※ 다수의 이용자가 공동으로 사용할 수 있는 인증수단은 인증기준에 부적합합니다. • 네이버·카카오 등 소셜계정 로그인도 로그인 편의 수단으로 사용할 수 있으나, 소셜계정 정보만으로 본인확인 및 다중인증 요건을 충족한 것으로 보기 어렵습니다. • 사업자 유형 및 문자발송 환경에 따라 다중인증 도입이 불가한 경우 대체통제 수단을 포함한 소명자료를 제출하여 심사받을 수 있습니다. ※ 도입이 불가한 사유 및 대체통제 수단은 서류·현장 심사 및 최종 심의에서 보완 및 거절될 수 있습니다. • 비인가자가 고객사 연동정보를 탈취하거나 임의 서버에서 발송 요청을 생성하지 못하도록 연동 주체를 강하게 인증하고 접근을 제한해야 합니다. • 사설발송 유형 중 솔루션(웹GUI 혹은 독립 구축형 소프트웨어)의 경우 웹페이지 발송과 동일한 인증 기준을 적용합니다. 【주의사항】 • 다중인증 예외는 원칙적으로 인정하기 어렵습니다. 폐쇄망 등 특수환경은 별도 소명자료와 보완통제 방안을 제출할 수 있으나, 수용 여부는 심사 과정에서 검토됩니다. • 고위험 계정 또는 관리자 계정은 이메일 OTP 등보다 강한 인증수단을 병행하는 것이 바람직합니다. • 고객사 내부 이용자에게 직접 다중인증을 적용하기 어려운 경우 연동 주체에 대한 인증 및 접근통제를 강화해야 합니다. 【증빙자료】 • 다중인증 설명자료 • 다중인증 화면 캡처 • 인증수단 등록·변경·재설정 이력 • 로그인 실패 횟수 제한 경고 및 차단 화면 캡처 • 소셜계정 로그인 연계 및 추가인증 흐름도 • 사설발송 유형에 대한 인증 소명자료 ※ 사설발송 유형 중 다중인증 적용 어려운 경우 대체통제수단 소명이 필요한 경우 제출

항목	3.5. 추가 인증 (발신 인증)
상세 내용	▶ 추가인증은 문자 발송 시 해당 발신번호와 발송 계정의 정당한 연계성을 확인하여 발신번호 도용과 대량 문자 남용을 방지하기 위한 절차이다. ▶ 추가인증은 반드시 매 발송 건마다 반복해야 하는 것은 아니며, 동일 세션·일정 시간 유지, 발신번호 변경·대량발송·접속환경 변경 시 재인증 등 사업자 자체 기준을 마련하여 운영이 가능하다. ▶ 사설발송 유형과 같이 이용자가 문자발송 웹페이지에서 직접 발송하지 않는 구조의 경우에도 발송자와 발신번호 간의 정당한 연계성을 확인할 수 있는 대체통제 수단을 마련하여야 한다.
주요 확인 사항	① 문자 발송 시 발신번호와 발송 계정의 정당한 연계성을 확인하는 추가인증 절차가 있는가? ② 추가인증 수단이 회원가입 및 발신번호 등록 과정에서 확인된 정보와 연계되어 있는가? ③ 유선번호·대표번호에 대해 ARS, 계정·서비스 연계 인증 등 대체 인증방식이 마련되어 있는가? ④ (필요시) 대량발송·발신번호 변경·접속환경 변경 등 위험조건에 따른 재인증 기준이 있는가? ⑤ (3.4. 다중인증, 3.5. 추가인증 공통) 사설발송 유형별 Agent, API Key, 인증서 등 발송 요청 인증수단이 관리되고 있는가? ※ Agent 고유 식별값 관리, API Key 관리, mTLS 등 서버 인증서, 그 외 대체 통제수단 ⇒ 발신번호 도용 방지와 발송자 추적관리 용이성을 확보하기 위한 추가인증 또는 이에 준하는 통제체계 운영
항목 해설	【설 명】 • 추가인증 수단은 다중인증과 동일하게 이용자 계정정보(휴대폰번호, 이메일 등)를 활용한 OTP 등 수단을 도입할 수 있습니다. ※ 다수의 이용자가 공동으로 사용할 수 있는 인증수단은 인증기준에 부적합합니다. • 무선발신번호는 SMS OTP 등 번호기반 추가인증 수단을 운영할 수 있습니다. • 유선번호 또는 대표번호는 ARS 음성 인증을 운영할 수 있습니다. ※ 인증받으려는 유선번호에서 사업자가 지정한 번호로 전화를 걸고, 시스템이 인입 발신번호와 등록 요청 발신번호의 일치 여부를 확인하여 인증 처리하는 방식은 ARS 기반 추가인증으로 운영할 수 있습니다. • 추가인증 완료 후 일정 시간 또는 동일 세션 내에서 인증 상태를 유지할 수 있으며, 사업자는 인증 유지 시간, 대량발송 등 기준을 자체적으로 정하고 그 기준과 재인증 절차를 문서화해야 합니다. • 사업자 유형 및 문자발송 환경에 따라 추가인증 도입이 불가한 경우 대체통제 수단을 포함한 소명자료를 제출하여 심사받을 수 있습니다. ※ 도입이 불가한 사유 및 대체통제 수단은 서류·현장 심사 및 최종 심의에서 보완 및 거절될 수 있습니다. • 사설발송 유형 중 솔루션(웹GUI 혹은 독립 구축형 소프트웨어)의 경우 웹페이지 발송과 동일한 인증 기준을 적용합니다. • 추가인증 도입이 불가한 경우 서비스를 이용하는 기업 고객사의 관리자 또는 담당자를 지정하여 전자결재, 콘솔을 통한 관리자 승인, 이메일 승인 등 확인(승인) 사실을 입증할 수 있는 방식으로 기능을 제공할 수 있습니다. ※ 사후승인은 이용자의 불법스팸 발송으로 인한 피해(발신번호 차단 등) 예방을 위한 조치로 활용될 수 있습니다. 【주의사항】 • 폐쇄망 등 특수환경은 별도 소명자료와 보완통제 방안을 제출할 수 있으나, 수용 여부는 심사 과정에서 검토됩니다. • 내용 수정이 불가한 템플릿, 인증번호, 정형화된 시스템 안내, 시스템 자동발송 등 이용자 개입이 없는 발송 건에 대해서는 인증을 생략할 수 있습니다. • 이용자의 서비스(쿠폰, 선물하기 등) 제공을 위한 발송 건에 대해서는 인증을 생략할 수 있습니다. 【증빙자료】 • 추가인증 설명자료 • 문자 발송 시 팝업되는 추가인증 화면 캡처 • (있는 경우) 재인증 기준(불법스팸 발송 방지계획서 작성) • 사설발송 유형에 대한 추가인증 대체통제수단 소명자료(필요한 경우)

2.4. 기록 관리의 적정성

항목	4.1. 이용자 로그 관리
상세 내용	▶ 이용자의 서비스 이용 과정에서 발생하는 접속, 인증, 발송, 과금 등 활동 기록은 이용자 식별과 책임 추적을 위한 필수 정보이다. ▶ 관련 법령에서 정한 최소 보관기간 이상 보관하되, 별도 기간이 없는 경우 1년 이상 보관해야 하며 분실·변조·삭제되지 않도록 안전하게 저장해야 한다.
주요 확인 사항	① 이용자 서비스 페이지 접속 로그를 보관하고 있는가? ② 회원가입·다중인증·추가인증 로그를 보관하고 있는가? ③ 계정·발신번호별 문자 발송 이력을 보관하고 있는가? ④ 과금 및 결제 이력을 계정별로 보관하고 있는가? ⑤ 로그가 삭제·변조되지 않도록 접근통제 및 백업이 이루어지는가? ⇒ 이용자 식별 및 사고 추적에 필요한 주요 로그를 관련 법령상 최소기간 이상 보관
항목 해설	【설 명】 • 접속 로그에는 계정, IP, 접속일시, 접속경로, 성공·실패 여부 등을 포함하는 것이 적절합니다. • 인증 로그에는 (다중, 추가)인증수단, 인증이력, 성공·실패 여부, 인증 대상 정보, 인증 요청 계정 등을 기록합니다. • 문자 발송 이력은 발송일시, 발신번호, 수신번호, 발송계정, 발송결과 등을 포함합니다. • 과금 이력은 요청일시, 결제수단, 결제금액, 주문번호, 승인번호, 처리결과 등을 계정과 연계하여 보관합니다. • 로그는 파일뿐 아니라 데이터베이스에 저장할 수 있으며, 주기적 백업 및 복구 가능성이 확보되어야 합니다. 【주의사항】 • 로그 저장 위치와 보관기간, 접근권한, 백업정책이 명확해야 합니다. 【증빙자료】 • 모든 로그 저장 기록(로그 기록별 저장된 파일 목록 캡처) • 로그 보관 정책

항목	4.2. 시스템 로그 관리
상세 내용	▶ 관리자 또는 시스템 운영자가 문자발송 시스템에 접속하여 수행하는 행위, 시스템 오류 및 장애, 개인정보 조회·수정·삭제 이력은 보안사고 및 책임 추적을 위해 보관되어야 한다. ▶ 문자발송 기능 수행 및 운영·관리와 직접 관련된 주요 시스템은 단순 관리자 페이지에 한정되지 않는다.
주요 확인 사항	① 문자발송 시스템 관리자 접속기록을 보관하고 있는가? ② 시스템 오류 및 장애 로그를 보관하고 있는가? ③ 개인정보 조회·수정·삭제 이력을 보관하고 있는가? ④ DB 서버, 인증 시스템, API 서버, 운영관리 시스템 등 주요 시스템 로그가 관리 대상에 포함되는가? ⑤ 로그 접근권한 및 삭제·변조 방지 조치가 마련되어 있는가? ⇒ 시스템 운영 및 개인정보 처리 관련 로그를 관련 법령상 최소기간 이상 보관
항목 해설	【설 명】 - 문자발송 시스템의 범위에는 발송 서버, 관리자 시스템, 인증 시스템, DB 서버, API 서버, 접근통제 시스템, 운영관리 시스템 등 문자 발송 기능과 직접 관련된 주요 시스템이 포함될 수 있습니다. - 시스템 로그에는 관리자 ID, 접속일시, 접속 IP, 수행행위, 대상정보, 결과, 장애 발생·복구 일시 등을 포함하는 것이 적절합니다. •(개인정보가 있는 경우) 개인정보 처리 이력은 조회, 수정, 삭제, 다운로드 등 행위별로 기록되어야 합니다. 【증빙자료】 - 관리자 페이지 로그만 보관하고 DB·API·인증 시스템 로그를 제외하면 보완이 필요할 수 있습니다. 【증빙자료】 - 모든 로그 저장 기록(로그 기록별 저장된 파일 목록 캡처)

항목	4.3. 로그 점검
상세 내용	▶ 사업자는 이용자 로그 및 시스템 로그의 이상 여부를 자체적으로 정기 점검하여야 하며, 점검 결과를 기록·보관하여야 한다.
주요 확인 사항	① 이용자 로그 및 시스템 로그를 월 1회 이상 정기적으로 점검하고 있는가? ② 로그 점검 결과를 기록·보관하고 있는가? ③ 이상징후 발견 시 후속조치 절차를 운영하고 있는가? ⇒ 로그의 생성·보관뿐 아니라 정기적인 검토 및 사후조치 체계 운영 여부 확인
항목 해설	【설 명】 - 로그 보관만으로는 충분하지 않으며, 사업자는 이용자 로그와 시스템 로그를 주기적으로 검토하여 이상여부를 확인하여야 합니다. - 로그 점검 결과는 점검일자, 점검자, 점검대상, 점검결과, 조치사항 등을 포함하여 기록·보관하여야 합니다. 【주의사항】 - 점검 결과만 작성하고 실제 로그와 연결되지 않으면 보완이 필요합니다. 【증빙자료】 - 로그 점검 양식 ※ 생성된 로그의 파일명과 파일사이즈를 확인할 수 있는 화면 캡처 ※ 누락여부 확인 ※ 누락 시 원인파악 및 조치내역

2.5. 조치의 적정성

항목	5.1. 조치 및 결과확인
상세 내용	▶ 문자 발송 서비스 이용자 중 일부가 불법스팸을 전송할 경우, 해당 행위에 대한 신속하고 적절한 조치를 취하는 것이 매우 중요합니다. ▶ 자체 모니터링, 외부 요청 등을 통해 스팸 의심 이력을 식별·기록하고, 실제로 이용 중단이나 해지 등 조치를 이행했는지를 확인하기 위해 마련되었습니다. ▶ 조치 이후 이력 보관이 이뤄지고 있는지, 이용자 고지 절차가 투명하게 진행되었는지 여부도 핵심 확인사항입니다.
주요 확인 사항	① 불법스팸 신고 내역 확인 절차 여부 ② 불법스팸 의심 건 발생 시 이용자에 대한 조치 절차 및 이력 관리 여부 ③ 조치 결과를 체계적으로 문서화하고 보관·관리하고 있는가? ⇒ 역무제공거부 근거로 조치내역을 보관하고 이용자에 고지
항목 해설	【설 명】 • 이용약관 또는 서비스 계약서에는 불법스팸 전송 시 서비스 중단, 제한, 해지 등의 조치를 할 수 있다는 내용이 포함되어야 합니다. • 내부 모니터링 또는 외부기관 통보를 통해 불법스팸 의심이 확인되면, 그에 대한 내부 조치 결과(예: 경고, 일시 정지, 계정 해지 등)를 문서화해 처리이력으로 남겨야 합니다. • 스팸 신고 접수 및 조치가 이루어졌을 경우, 이용자에게 즉시 이메일, 문자, 알림창 등을 통해 조치 사유를 명확히 안내해야 합니다. 【주의사항】 • 조치 기준은 약관·계약서·불법스팸 발송 방지계획서 등 내용과 일치해야 합니다. • 조치 내역은 사후 민원, 수사기관 요청, 인증점검 시 확인할 수 있어야 합니다. 【증빙자료】 • (상위사업자 또는 외부기관 공유) 스팸신고 확인 및 이에 대한 조치 절차 ※ 해당 절차는 불법스팸 발송 방지계획서에 포함되어야 하며, 해당 내용을 증빙자료로 제출 • (있는 경우) 신고내역(이용자, 발신번호) 별 조치결과 이력

항목	5.2. 금칙어 등 차단 체계(스팸 필터링) 운영
상세 내용	▶ 불법스팸을 사전에 차단하기 위해서는 문자 내용 중 포함된 특정 금칙어, URL 등 위험 요소를 자동으로 탐지하고 차단하는 체계가 필요합니다. ▶ 사업자가 스팸 의심 요소를 사전에 필터링할 수 있는 차단 체계를 실시간으로 적용하는지 여부를 점검합니다.
주요 확인 사항	① 문자 내용 중 금칙어(키워드, URL, 전화번호 등)가 포함된 경우 차단하는 체계가 구축되어 있는가? ② 공유된 금칙어를 차단 체계에 적용할 수 있는가? ③ 차단 체계 작동 여부 및 탐지 로그를 확보하고 있는가? ⇒ 금칙어 등 차단 정보는 외부기관을 통해 전달받아 적용할 수 있어야 하며, 다중 조합 필터링 체계를 운영 (문자 내용을 1개 이상(최대 5개)의 차단정보 조합으로 구성하여 탐지 및 차단)
항목 해설	【설 명】 ① 문자 전송을 요청받을 때, 문자 내용에 포함된 키워드, URL, 전화번호 등 위험 요소(금칙어)를 자동으로 탐지할 수 있어야 합니다. • 한국인터넷진흥원 등 외부기관을 통해 공유받은 차단 정보를 적용하여 스팸 필터링을 운영해야 합니다. • 차단정보는 다중으로 구성될 수 있어야 하며, 단일차단정보로는 키워드, URL, 전화번호 등을 포함한다. ② 금칙어가 탐지되었을 경우 시스템은 자동으로 해당 발송을 즉시 차단하거나 보류하고, 관리자 승인 요청 또는 경고 안내 메시지를 표시해야 합니다. ③ 실제로 차단된 이력은 기록으로 남아 있어야 하며, 로그 파일 또는 시스템 내에서 확인할 수 있어야 합니다. • 이력은 사후 점검, 이용자 소명 요청 대응, 현장 점검 대응 시 근거자료로 제출해야 합니다. 【증빙자료】 • 문자 발송 시 금칙어 차단 체계 운영 화면 캡처 • 차단 체계 운영 현황 및 탐지/차단 결과 로그 • (있는 경우) 차단/보류 발생 시 안내 팝업 또는 메시지 화면 • 금칙어(차단정보) 관리 리스트 및 주기적 업데이트 내역

불법스팸 발송 방지 계획서

회사명
대표자
작성 일자 20 년 월 일
제출 목적 전송자격인증제 신청

「전기통신사업법」 제22조의 11 및 관련 고시에 따른 전송자격인증 기준을 준수하고, 불법스팸 발송을 사전에 방지하기 위한 체계적인 계획을 수립하고 이를 성실히 이행할 것을 약속합니다.

1. 불법스팸 방지 전담조직 구성 및 운영 계획

불법스팸 방지 관련 업무의 책임 있는 이행을 위해 아래와 같이 전담 조직을 구성하고 운영합니다.

1.1. 전담 조직 구성 현황

구분	내용
불법스팸 담당 조직명	
전체 조직도(첨부)	[첨부. 불법스팸 담당 조직도]를 첨부하며, 해당 조직의 위치를 표시
총괄 책임자 정보	성명: / 직함: / 소속부서: / 연락처:
불법스팸 담당 인원 수	총 [숫자] 명

1.2. 전담 조직의 운영 계획

불법스팸 방지 업무 전반에 걸친 역할과 책임(R&R)을 명확히 하고, 신고 접수 및 처리에 필요한 충분한 권한을 부여하여 신속하고 체계적으로 대응합니다.

구분	주요 임무 및 역할	주관 부서
총괄 책임자	불법스팸 방지 정책 수립 및 최종 결정, 법적 대응 총괄	
운영/관리 담당	스팸 신고 접수 및 사실 조사, 이용제한 조치 실행 및 통보	
기술/보안 담당	이상징후 모니터링 시스템 운영 및 개선, 발송 차단 필터링 관리	

2. 불법스팸 대응(업무별 세부 프로세스 및 방법)

불법스팸 신고 접수 및 이상징후 탐지 시 지체 없이 조치하기 위한 세부 프로세스는 다음과 같습니다.

2.1. 불법스팸 신고 내역 확인 및 대응

구분	세부 내용
신고 내역 확인 주기	신고 접수 후 [숫자] 시간 이내 (최대 24시간을 초과하지 않음)
신고 접수 채널	[웹사이트, 이메일, 고객센터 전화번호 등 구체적으로 명시]
신고 처리 프로세스	① 접수 및 기록 → ② 발송 이력 및 내용 사실조사 → ③ 이용제한 조치 실행 및 발송자 통보 → ④ 신고인에게 처리 결과 통보(처리 완료 후 [숫자] 시간 이내 등)

2.2. 가입자(이용자) 이용 제한 세부 사항

구분	기준 및 기간	통보 방법 및 내용
이용 정지 기준	1. 불법스팸 신고 건수가 [숫자] 회 이상 접수되었을 경우 2. 이상징후 모니터링 시스템에서 [구체적인 기준] 이상 탐지되었을 경우	이메일, SMS 등을 통해 [이용 정지 사유], [정지 기간], [이의제기 방법]을 명시하여 통보
이용 정지 기간	최초 위반 시 [기간] 정지 (예: 7일)	
탈퇴(영구 해지) 기준	1. 이용 정지 기간 중 재차 불법스팸을 발송한 경우 2. 불법스팸을 3회 이상 상습적으로 발송한 경우 3. [구체적인 기준 (예: 법원/수사기관 등 요청)] 에 해당하는 경우	탈퇴 처리 사유 및 일자를 명시하여 통보

2.3. 사업자(하위 특부가통신사 등) 이용 제한 세부 사항

당사와 계약 관계에 있는 사업자가 불법스팸을 발송한 경우, 연대 책임을 묻고 하위 사업자 관리를 위해 다음과 같이 제재합니다.

구분	제재 기준	제재 기간 및 방법
계약 해지/해지 기준	1. 계약된 하위 사업자의 이용제한 비율이 [비율]% 를 초과할 경우 2. 중대한 불법스팸 발송으로 당사에 [구체적 피해 내용] 이 발생한 경우	[기간] 정지 후 소명 기간을 부여하며, 소명이 불충분하거나 재차 위반 시 계약 해지
하위 사업자 관리	[하위 사업자 관리 및 제재 방식에 대한 구체적인 내용을 기술] 예) 하위 사업자별 스팸 발송 이력 정기 공유, 사전 교육 이수 의무화, 월별 품질 평가 등	

3. 이상징후 모니터링 및 재발 방지 계획

3.1. 이상징후 모니터링 체계 및 방법

문자 발송 패턴의 급격한 변화를 실시간으로 탐지하고, 담당자에게 즉시 알람을 전송하여 선제적으로 불법스팸을 차단합니다.

구분	모니터링 상세 내용	담당자 알람 방법
야간 발송 모니터링	[구체적인 야간 시간대]에 발송량이 [기준]을 초과하는 경우	[알람 방법: SMS, 이메일, 전용 메신저 알람 등]
급증 발송량 확인	이전 [일별/월별/분기별] 대비 발송량이 [비율]% 이상 급증하는 계정을 실시간 탐지	[알람 방법: SMS, 이메일, 전용 메신저 알람 등]
키워드 및 패턴 모니터링	대출, 도박, 성인 등 금치어 포함 비율 및 URL 포함 비율 등 비정상 패턴을 지속적으로 감지	

3.2. 재발 방지를 위한 대응 방안

동일 이용자 또는 동일 계정이 반복적으로 불법스팸을 발송하는 경우 강력한 대응 조치를 적용하여 재발을 원천적으로 방지합니다.

상황	대응 방안(구체적 프로세스)
해킹/도용 사유로 해제 후 재발	해킹/계정 도용을 사유로 이용제한이 해제 처리된 이용자가 추가적으로 1회 이상 불법스팸을 발송할 경우 [조치: 영구 차단 및 서비스 이용 불가] 조치
상습 위반자 처리	이용 정지 조치 후 재가입 또는 명의만 변경하여 재차 위반 시 [조치: 명의와 관계없이 IP 및 기타 식별정보 기반의 영구 차단] 조치
재발 방지 서약/교육	이용 정지 해제 전, 해당 이용자로부터 [문서명: 예] 재발 방지 서약서] 또는 시스템 개선 계획서를 징구하는 절차를 의무화

4. 임직원의 불법스팸 방지를 위한 교육 계획

임직원의 불법스팸 관련 법규 이해도를 높이고 준수 의식을 확립하기 위한 정기 교육을 다음과 같이 실시합니다.

구분	내용
교육 대상	불법스팸 관련 업무 담당자 및 전 임직원
교육 주기	최소 [분기별/반기별] 1회 이상
교육 방법	[교육 방법: 온라인 교육 시스템, 정기 회의 시 의무 교육, 외부 전문가 초빙 등]
교육 내용	1. 「정보통신망법」 및 「전기통신사업법」 등 관련 법규 이해 2. 불법스팸 유형 및 최신 동향 공유 3. 사내 불법스팸 대응 프로세스 및 지침 숙지
교육 결과 관리	교육 이수 여부 및 결과를 기록하고 [기간] 동안 보관 (증빙 자료로 활용)

5. 계약 관계에 따른 불법스팸 방지 계획

5.1. 웹페이지 발송 서비스 및 이용 약관 관리

당사의 서비스를 통해 메시지를 발송하는 모든 이용자가 불법스팸을 발송하지 않도록 계약 및 약관에 관련 내용을 명확히 명시합니다.

- o 이용 약관 명시: 이용 약관에 ‘불법스팸 발송 금지’ 조항 및 이를 위반할 경우 ‘서비스 이용 제한(정지/해지)’ 조항을 명확하게 포함합니다.
- o 경고 문구 게시: 서비스 가입/신청 단계 및 발송 페이지에 불법스팸 관련 법규 위반 시 처벌받

을 수 있음을 고지하는 경고 문구를 게시합니다.

o 발송 전 확인: 메시지 발송 전(수신 동의 여부 확인 절차, 광고성 정보 표기 의무 안내 등) 필수 확인 사항을 안내하고 서약하도록 합니다.

5.2. 외부 계약 관계(ASP/재판매 등)에 대한 관리

외부 시스템 연동 또는 서비스 재판매 등 계약 관계에 있는 모든 사업자에게도 불법스팸 방지 의무를 부과하고 관리합니다.

o 계약서 반영: 모든 관련 계약서에 불법스팸 발송 시 **계약 해지** 및 **손해 배상** 책임 등을 명확히 명시합니다.

o 정기 점검: 계약 사업자의 불법스팸 방지 이행 여부를 (주기)로 점검하고, 미흡 사항 발견 시 개선을 요구합니다.

o 정보 공유: 불법스팸 신고 접수 및 조치 결과를 계약 사업자와 신속하게 공유하여 연쇄적인 불법스팸을 방지합니다.