# GME 고객민원 및 금융사고 대응체계관련 자료

2022-06-29

㈜글로벌머니익스프레스

# 목차

I. GME 금융사고 대응 매뉴얼

II. GME 민원 및 분쟁처리절차

III. 국가별 고객응대 채널 운영 현황

IV. 비상계획

# I. GME 금융사고 대응 매뉴얼

## 1. 보고대상

√ (전산장애사고) 정보처리시스템 또는 통신회선 등의 장애로 10분이상 전산업무 지연 및 중단되거나 전산자료 및 프로그램 조작과 관련된 금융사고

√ (IT보안사고) 전자적 침해행위로 인해 정보처리시스템에 사고, 이로 인해 이용자가 금전적 피해를 입었다고 금융기관에 통지한 경우

√ (전자금융피해사고) 전자금융법 제9조제1항의 규정에서 정하는 사고(접근매체 위·변조 또는 정보통신망 등에 침입하여 부정한 방법으로 취득한 접근매체의 이용으로 발생하거나 계약체결이나 거래지시의 전자적 전송이나 처리 과정에서 발생한 금전사고)

√ (기타 금융사고) 상기 외 기타 금융사고 발생시

## 2. 보고방법

전자금융사고 대응시스템(EFARS)을 통해 보고하고 최초보고, 중간보고 및 종결보고로 구분

* FINES금융정보교환망(fines.fss.or.kr) - 전자금융사고대응 - 보고서 작성

√ 최초보고 : 사고 인지 후 즉시(1영업일 이내) 실시

√ 중간보고 : 최초보고의 내용을 보완할 필요가 있는 경우 신속 보고하고, 사고 인지일로부터 조치완료시까지 2월 이상 소요될 경우 2월 이내에 실시하며 종료시까지 6개월마다 실시

√ 종결보고 : 피해금액에 대한 배상조치가 완료되거나 사고조치 등이 완료

## 3. 긴급상황시 최초보고 간소화

사실관계, 피해금액 등이 확정되지 않거나 긴급한 사고대응 등으로 최초보고 기한 내(인지 후 1영업일) 정확한 사고보고가 곤란한 경우 최초보고시 인지시점, 사고 개요 등만

간략 보고

☞ 사실관계 등이 확정되는 대로 중간보고를 통해 정확한 사고내용을 재보고

### 4. 보고절차의 간소화

최초보고시 사고대응 조치 등을 완료한 경우 종결보고 생략 가능

* 예) 10분간 전산장애가 발생하였으나 즉시 원인파악 및 대응조치를 완료

사고금액이 3억원 미만인 전자금융피해사고는 월 1회 취합 보고할 수 있도록 최초보고 시기를 조정

☞ 최초보고에 한하여 매월 발생한 사고를 취합하여 익월 15일 까지 일괄 보고 가능

☞ 다만, 사고금액이 3억원 이상인 경우 또는 IT보안사고나 전산장애 사고와 연계된 금전사고*의 경우 즉시 보고

* 예) GME에 대한 전자적 침해행위로 고객 정보가 유출되었고, 동 정보를 이용한 2차 금전사고가 발생한 경우

☞ ①IT보안사고, ②전산장애 사고, ③전자금융피해사고에 대한 중간 종결보고는 기존과 동일하게 건별 보고만 가능

### 5. 사고보고 대상 정비

전자금융피해사고 중 사고금액이 100만원 미만의 경미한 사고는 사고보고 대상에서 제외

☞ 다만, IT보안사고 또는 전산장애 사고와 연계된 금전사고는 IT보안사고 등과 연결선상에 있는 것으로 보아 사고금액에 무관하게 사고보고 대상에 포함(최초보고시 즉시보고)

* 예) GME에 대한 전자적 침해행위로 고객 정보가 유출되었고, 동 정보를 이용한 2차 금전사고가 발생한 경우

☞ 원인미상인 경우에도 동일한 기준을 적용하되, 조사결과 보고 대상 여부가 변경되면 즉시 보고 또는 보고회수를 통해 조정

| 사고금액 | IT보안·장애사고와 연계 여부* | 사고보고대상 여부 | 최초보고 방법 |
|---|---|---|---|
| 100만원 미만 | X | X | 미보고 |
| | O | O | 즉시보고 |
| 100만원 이상 3억원 미만 | X | O | 일괄보고 |
| | O | O | 즉시보고 |
| 3억원 이상 | - | O | 즉시보고 |

* IT보안사고 또는 전산장애 사고와 연계되어 발생한 2차적 금전사고

전산장애 사고 중 대고객 전자금융서비스에 영향이 없는 GME 자체 내부용 시스템의 장애는 사고보고 대상에서 제외

* GME 내부직원을 위한 이메일 등 인트라넷시스템 및 관련 네트워크 등

☞ 대고객용이긴 하나 단순 정보 제공 GME 웹페이지, 금융상품 이외의 서비스(마케팅 이벤트 등) 등의 장애도 보고대상에서 제외

## 6. 전자금융사고별 사고보고 기준

### ① 전산장애 사고

□ 10분 이상 전산업무 지연 및 중단

◦ (대상) 대고객 금융상품 및 서비스 제공 관련 시스템

.

전산자료 및 프로그램 조작과 관련된 금융사고 발생시

◦ (대상) 전자금융거래 관련 전산자료 또는 대고객 금융상품 및 서비스 제공 관련 프로그램

◦ (범위) 조작의 고의성과 상관없이 보고

- 단, 업무 처리과정에서 일상적·반복적으로 발생하는 사고로서 고객이 인지하지 못했거나 피해가 발생하지 않는 경우는 제외

### ② IT보안사고

□ 전자적 침해행위로 인해 정보처리시스템에 사고가 발생하거나 이로 인해 이용자가 금전적 피해를 입었다고 금융기관에 통지한 경우

◦ 전자금융기반시설에 대해 해킹, 컴퓨터 바이러스, 논리폭탄 등의 공격이 발생하여 전산업무 중단·지연, 정보유출, 금전사고 등 GME의 업무 또는 GME 고객에 피해가 발생하거나

* 전산장애 사고와 달리 대고객서비스 관련 시스템이 10분 이상 중단·지연되는 것을 요건으로 하지 않고, 모든 시스템에 대한 중단·지연 사고 발생시 사고보고를 실시해야 함

- 동 사고와 관련하여 이용자에게 금전피해(2차 금전사고)가 발생한 경우 사고보고 대상에 해당함

◦ 전자적 침해행위가 있었으나 사고가 발생하지 않은 경우 사고 보고 대상에서 제외

- 다만, EFARS를 통한 사고보고를 실시하지 않더라도 추가적인 침해행위 및 피해발생을 예방하기 위해 침해행위 발생 사실을 금융당국과 금융보안원에 유선 등으로 통지해야 함

# II. GME 민원 및 분쟁처리절차

# GME 민원 및 분쟁처리절차

GME REMITTANCE

# GME 민원 및 분쟁처리 절차

## 1. 목적

GME 해외송금서비스를 이용하는 고객이 제기하는 정당한 의견이나 불만을 반영하고 동 서비스의 이용과 관련하여 손해가 발생한 고객에 대하여는 이를 배상할 수 있는 절차를 마련해 줌으로써 GME의 대고객 신뢰도를 제고한다

## 2. 민원 및 분쟁 사항의 접수 방법

❑유선전화: 1588-6864(음성녹음)
❑GME 홈페이지(www.gmeremit.com)내 'Contact Us하부 메뉴접속'
❑영업점 '고객의 소리' 함(민원신청서 지점창구비치)
❑우편

■신청사유 작성과 관련하여 6하 원칙에 따라 기술하도록하고 개인정보제공동의(비동의시 민원처리 불가) 민원신청과 관련하여 민원당사자, 이해관계인 및 사실관계를 입증하는 경우 본인 실명확인증표 사본서류, 대리인이 신청하는 경우 본인의 위임장 <민원신청서식> 및 인감증명서를 첨부하고 기타 사실관계를 입증하는 서류 사본을 첨부토록 안내한다.

■안내문구

| |
|---|
| **민원(불만) 및 칭찬, 건의는 개인정보보호법 제15조, 제 24조, 제24조2에 따라 고객님의 동의가 필요합니다** |

## 3. 민원처리 기구

❑ 구성
■민원처리 책임자: 대표이사 성종화(010-4163-7562)
■민원처리 담당자: 경영지원팀장 홍지현(010-8787-1011)

## 4. 민원서류의 접수 및 접수사실 통지

❑민원을 접수한 영업점 및 본부부서는 민원서류를 접수하는 즉시 민원접수 사실, 민원담당 전화번호 등을 민원신청인에게 문서, 팩스, 전자우편(e-Mail), 문자메시지, 녹취전화 등 입증이 가능한 방법으로 통지한다.
❑민원처리 담당직원은 민원접수 사실 통지후 민원신청인과 전화통화 등의 방법으로 사실 관계 확인 및 처리 방향에 대한 사전 협의를 실시할 수 있다.

## 5. 민원처리 기한

민원(불만) 및 제안사항에 대한 조치결과는 고객에게 유선 또는 이메일로 신속히 답변하여야하며, 민원사항에 대해서는 접수사실을 확인하는 1차 답변 후 14영업일 이내에 조사 및 처리결과를 회신한다.

## 6. 민원 철회

❑민원신청인은 민원 처리가 종결되기 전에 그 신청내용을 변경할 수 있으며, 신청을 철회 또는 취하할 수 있다.
❑민원의 철회 또는 취하는 민원신청인이 문서, 팩스, 인터넷 또는 녹취 전화 등 입증이 가능한 방법으로 한다.

## 7. 민원 진행사항 및 처리 결과의 통지

**❑진행상황 통지**
민원신청인으로부터 민원처리에 대한 진행상황 통지요청이 있는 경우 별지의 서식을 통해 팩스(fax), 전자우편 또는 녹취 전화 등으로 안내한다

**❑처리결과통지**
민원은 접수일로부터 14영업일 이내에 처리하고 결과를 통지요청이 있는 경우 별지 서식을 통해 팩스, 전자우편으로 안내한다.

## 8. 분쟁처리 절차

### ❑ 정당한 의견

■ 의견 접수 후 분쟁처리기구(분쟁처리 책임자: 대표이사, 분쟁처리 담당자:영업관리지원팀장) 통하여 회사의견 결정 후 15일 이내에 통보한다

■ GME 업무절차에 조기 반영 및 그 결과를 민원인에게 이메일 및 우편 또는 전화로 통보한다.

### ❑단순 불만 사항

고객 ⇒ 불만사항 접수 (유선전화, 홈페이지 등) ⇒ 분쟁처리 담당자 확인 ⇒ [ 해결 ⇒ 분쟁처리 결과 책임자 보고 / 미해결 ⇒ 분쟁처리책임자 해결 ]

⇒ 분쟁처리결과 고객 통지 (이메일 및 우편)

### ❑ 손해배상 요구 사항

고객 ⇒ 불만사항 접수 (유선전화, 홈페이지 등) ⇒ 분쟁처리 담당자 확인 ⇒ 분쟁처리기구 보고 ⇒ [ 해 결 / 미해결 ]

⇒ 분쟁처리결과 고객 통지 (이메일 및 우편) ⇒ 분쟁조정 신청 (금융감독원 또는 한국소비자원)

# III. 국가별 고객응대 채널 운영 현황

| Corridor | Phone No | PIC | CS Off Days | Operation Hours (KST) |
|---|---|---|---|---|
| Nepal | 1811-2934 | Sandip<br>Sunitat<br>Dil<br>Rabin | 7 days working | 10:15 - 23:45 |
| | 010-2959-6864 | Rajesh | 7 Days working | 10:00 - 23:59 |
| | 010-2954-6864 | Sunesh | 7 Days working | 10:00 - 23:59 |
| | 010-6584-6864 | Dinesh (Loan) | 7 Days working | 09:00 - 23:59 |
| Cambodia | 1811-2948<br>02-2138-6427 | Kongly<br>Kimleang<br>Shopheaktra | 7 Days working | 09:00 - 23:00 |
| | 010-2971-6864 | Leaphy | 7 Days working | 10:00 - 23:59 |
| | 010-7221-6864 | Samedi | 7 Days working | 10:00 - 23:59 |
| | 010-2962-6864 | Boren | 7 Days working | 10:00 - 23:59 |
| | 010-7487-6864 | DayDay | 5 Days Working | 10:00-18:59 |
| | 010-3077-6864 | Bo Ren / Eunjeong | 7 Days working | 10:00 - 23:59 |
| Sri Lanka | 1811-2935 | Shehani | Friday | 10:00 - 20:00 |
| | | Sandaruwan | Thu | 2:00 - 11:59 |
| | 010-2837-6864 | Sachini | 5 Days working | 11:00-7:00 |
| | 010-2950-6864 | Senarath | 7 Days working | 10:00 - 23:59 |
| | 010-2965-6864 | Mali (Loan) | 5 Days working | 09:00 - 23:59 |
| Vietnam | 1811-2937 | Thu Hong | 7 Days working | 09:00- 23:00 |
| | 010-9549-6864 | Rey | 7 Days working | 10:00-23.59 |
| | 010-9889-6864 | Enoza | 7 days working | 10:00-23:59 |
| | 010-2930-6864 | Ahn | Tue & Wed | 10:00 - 23:59 |

# IV. 비상계획

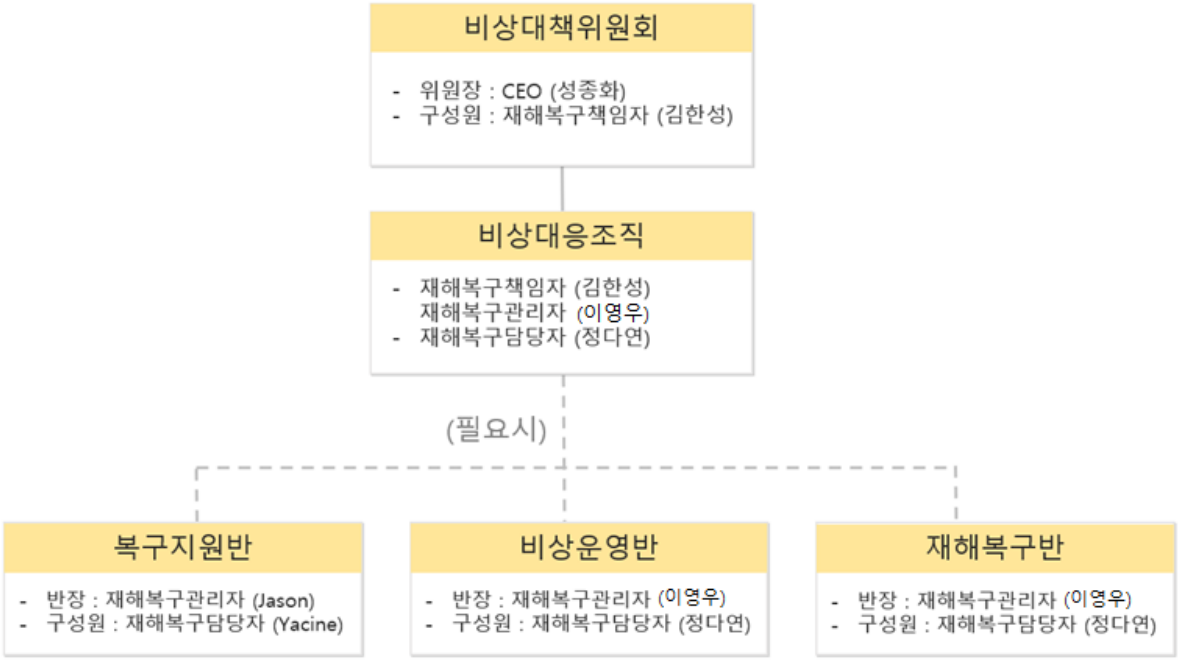
### 비상 계획 목적

이 지침은 장애 또는 재해 발생시 서비스 및 업무가 중단되지 않도록 하기 위해 서비스 연속성 확보, 비상지원인력확보, 재해복구 및 비상대응훈련 등 필요한 제반사항의 기준을 정함을 목적으로 한다. 이 지침에서 사용하는 용어의 정의는 다음과 같다.

① '장애'는 IDC, 서버실 및 장비실의 정보시스템, 통신회선 등이 그 본래의 기능을 상실하여 더 이상 IT 서비스를 제공할 수 없는 상태를 말한다.
② '재해'는 자연적, 인위적 재난 또는 위해로 인하여 IDC, 서버실 및 장비실의 정보시스템을 가동할 수 없거나 IT 관련 사무실 공간에서 더 이상 업무를 수행할 수 없는 상태를 말한다.
③ '비상사태'라 함은 예기치 못한 재해 발생으로 정보시스템의 운영이 일정시간 가동되지 못하여 업무수행에 치명적인 영향을 초래하는 경우나, 장애사태가 매우 심각하여 장애대책만으로 장애를 해결하기 힘든 경우를 말한다.

### 재해 복구 조직 및 역할

1) 조직도




1) 역할

① 비상대책위원장은 상황Ⅲ, 상황Ⅳ 및 상황Ⅴ 이외에도 중대한 비상사태라고 판단되는 경우 비상대책위원회를 소집할 수 있다.

② 비상대책위원장은 상황Ⅲ, 상황Ⅳ 및 상황Ⅴ의 경우 재해를 선포하고 대체장소로의 이동을 결정한다.

③ 비상대책위원회는 재해복구와 관련한 사항을 심의 및 의결한다.

| 반 | 역할 | 구성원 | 정책 근거 |
|---|---|---|---|
| 복구지원반 | 비상조치, 피해평가, 자원조달, 법률지원, 긴급예산수립 및 대외기관 통보, 언론대응 등의 역할을 담당 | 반장: 재해복구관리자<br>반원: 재해복구담당자 및 관련 부서의 장이 지정한 재해복구담당자 등 | 재해복구책임자는 비상사태가 발생해 재해의 공지 및 복구의 가동이 필요한 단계에서 비상대책위원회를 보좌하고 재해복구의 지원을 위해 다음 각 호와 같이 복구지원반을 운영할 수 있다. |
| 비상운영반 | 대체장소에서의 비상운영에 필요한 역할과 복구활동 지원의 역할을 담당 | 반장: 재해복구관리자<br>반원: 재해복구담당자 및 관련 부서의 장이 지정한 재해복구담당자 등 | 재해복구책임자는 비상사태가 발생해 대체장소의 비상운영이 필요한 단계에서 핵심 시스템의 가동을 위해 다음 각 호와 같이 비상운영반을 운영할 수 있다. |
| 재해복구반 | IT 인프라의 복구와 관련한 역할을 담당 | 반장: 재해복구관리자<br>반원: 재해복구담당자 및 관련 부서의 장이 지정한 재해복구담당자 등 | 재해복구책임자는 비상사태에 따른 대체장소의 비상운영을 종료하고 정상적인 정보시스템의 업무를 재개하기 위해 다음 각 호와 같이 재해복구반을 운영할 수 있다. |

2) 재해복구 정책

① 재해복구책임자는 재해복구 전략, 비상대응조직 역할, 보고체계, 비상사태별 대응 및 복구계획, 모의훈련계획, 유지보수계획, 비상연락체계 등의 재해복구 정책을 수립한다.

② 재해복구책임자는 재해복구 정책 및 전략의 실효성을 검토하기 위해 연 1회 비상대응 모의훈련계획을 수립해야 한다.

③ 재해복구책임자는 경영환경 변화 및 조직구조 개편 등 주요 변동사항이 발생할 경우 복구목표시간, 복구시점 및 복구우선순위를 검토하여 변경사항을 재해복구 정책에 반영한다.

④ 재해복구책임자는 '업무영향분석(BIA, Business Impact Analysis)'을 통해 복구목표시간(RTO, Recovery Time Objective) 및 복구시점(RPO, Recovery Point Objective)을 정의한다.

⑤ 재해복구관리자는 핵심업무에 대해 정상적인 업무수행을 할 수 없는 경우를 대비해 대체수행자를 지정하여 운영한다.

⑥ 재해복구관리자는 장애 또는 재해 발생으로 인하여 업무중단이 발생하는 경우를 대비해 각

업무별 피해규모 및 업무중요도를 분석하여 최소 복구목표시간, 복구시점 및 복구우선순위를 산정한다.

⑦ 재해복구관리자는 복구목표시간, 복구시점 및 복구우선순위를 '정보시스템 복구우선순위'에 작성하여 관리한다.

3) 비상대응조직 체계

① 재해복구책임자는 상황I, 상황II인 경우 비상대책위원회의 소집을 요청할 수 있다.

② 비상대책위원장은 상황III, 상황IV, 및 상황V인 경우 비상대책위원회를 소집한다.

③ 재해복구책임자는 비상사태가 발생하는 경우 정보시스템의 비상대응조치 및 업무처리 등을 위해 '복구지원반', '비상운영반' 및 '재해복구반(이하 '비상대응조직등'이라 한다)'을 운영할 수 있다.

④ 각 부서의 장은 재해복구책임자가 각 부서의 장에게 비상대응조직등에 대해 다음 각 호와 같이 재해복구담당자 인력을 요청하는 경우 협조해야 한다.

- 언론대응 인력
- 홍보활동 인력
- 시설 설치 및 이동 인력
- 예산관리 인력 등

**비상 상황 구분**

재해복구책임자는 비상사태의 장애 또는 재해 발생 상황을 다음 각 호와 같이 구분하여 재해복구 대책을 운영한다.

- 상황Ⅰ : 부분 또는 일시적 장애가 발생해 30분 이내에 복구가 가능한 통상적인 상황
- 상황II : 소규모의 재해가 발생해 3시간 이내에 복구가 가능한 상황
- 상황III : 중규모의 재해가 발생해 3시간 이상 IT서비스가 불가능하여 대체장소로 이동이 요구되는 상황
- 상황IV : 대규모의 재해 및 재난으로 즉각적인 대체장소로의 이동이 필요한 상황
- 상황V : 상황III 및 상황IV를 제외한 인위적인 재해가 발생한 상황(예 : 노사분규, 파업 등)

**재해 복구**

- 백업 목표: RPO(Recovery Point Objective) 1일, RTO(Recovery Time Objective) 1.5일
- 복구 형태: Cold Site

1) 백업자료 복구기준

| | |
|---|---|
| 정보시스템 및 데이터 | - 재해복구관리자는 장애 또는 재해가 발생하는 경우 즉시 활용할 수 있도록 중요 정보를 백업 정책에 따라 백업해야 한다.<br>- 운영담당자는 백업 소산장소로부터 인계 받은 백업 자료를 정보시스템 및 데이터 복구 절차에 따라 복구해야 한다.<br>- 운영담당자는 시스템 복구 시 하드웨어, 운영체제(OS)를 포함한 정보시스템, 소프트웨어 및 데이터베이스 복구를 포함한다. |
| 응용프로그램 | - 응용프로그램담당자는 복구우선순위에 따라 응용프로그램 복구를 수행해야 한다. 복구 작업을 완료한 후 서비스를 실시하기 이전에 복구의 정확성•신뢰성을 검증해야 한다. |
| 네트워크 | - 네트워크담당자는 작업순서, 네트워크 구성도 등 복구절차를 수립해 복구를 수행해야 한다.<br>- 네트워크담당자는 기본적으로 네트워크 연결을 위한 네트워크 장비를 미리 확보해 재난에 대비한다. |

2) 상황 별 재해복구

재해복구책임자는 장애 또는 재해의 상황에 따른 IT재해복구를 다음 각 호와 같이 수행한다.

- 상황Ⅰ, 상황Ⅱ: 대체장소로의 이동이 불필요한 상황으로 신속한 복구와 보고를 통하여 재해복구를 처리
- 상황Ⅲ, 상황Ⅳ: 대체장소로의 이동이 필요한 상황으로 대체장소로 이동을 준비하는 등의 재해복구를 수행
- 상황Ⅴ: 비상대책위원회의 의결에 따라 대체장소로 이동을 실시

3) 재해복구 절차

① 신규 가상화 서버 수급

② 소산 백업된 외장하드를 가지고 이동

③ 신규 가상화 서버에 VM 설치

④ OS 설치

⑤ 네트워크 설정

⑥ 기능 및 프로그램(MSSQL, SSMS, 닷넷, IIS) 설치

⑦ 소산 백업된 데이터를 신규 장비에 복원

⑧ 소산 백업된 앱/웹 퍼블리싱

**재해해제 및 후속조치**

- 비상대책위원장은 정보시스템이 정상으로 복구되는 경우 재해해제를 선포하고 비상대응조직을 해산시킨다.
- 재해복구관리자는 비상사태 시 수행하였던 비상대응 조치 및 절차 등에 대해 개선이 필요한 경우 정보보호 담당부서에 IT재해복구 운영 지침의 변경을 요청할 수 있다.
- 재해복구담당자는 정보시스템 복구 후 침해사고(장애) 예방, 발생, 대응결과 보고서를 작성하고 보고체계에 따라 정보보호최고책임자에게 보고한다.

**모의 훈련**

재해복구관리자는 재해복구계획이 적절하게 작동하는지를 검토하기 위해 연 1회 이상 모의훈련을 실시한다.

1) 모의훈련 계획

재해복구관리자는 모의훈련을 실시하는 경우 다음 내용을 포함하는 재해복구 평가 모의훈련을 계획서를 작성하여 최고경영자의 승인을 받고 관련부서에 공지한 후 실시한다.

- 모의훈련을 실시하는 목적
- 재해복구계획에 대한 실질적인 평가
- 재해복구계획에서 세부적으로 기술된 작업•절차가 복구 목표 달성에 필요한 실제 작업•절차와 일치하는 것에 대한 보장

- 재해복구계획의 변경을 위해 필요한 요구사항 파악
- 재해복구계획이 실제로 가동되었을 경우 제대로 작동할 것에 대한 보장
- 훈련 유형의 결정
- 구조적 검토(Walkthrough): 부서나 혹은 부서원들이 여러 시나리오를 가정하면서 논리적인 토론을 거쳐 재해복구계획의 타당성이나 실증성을 검증하는 방법
- 기술적 구성요소 시험: 재해복구계획에 명시된 기술적 구성요소를 시험하는 것으로 사용자가 참여하지 않은 상태에서 진행하는 방법
    - 예시1: 외부에서 이루어진 재해 복구 계약의 실행 여부 시험
    - 예시2: 예비 공간에 비상 접근 가능 여부 시험
    - 예시3: 예비공간에 전화 서비스 설치 가능 여부 시험 등
- 업무 구성요소 시험: 업무 프로세스나 기능이 복구되는지 여부를 시험하는 것으로 관련된 사용자가 참여하여 진행하는 방법
- 모든 구성 요소를 포함한 시험
- 훈련계획 수립 시 고려할 사항
- 훈련에 참가하는 부서 및 인원
- 훈련을 위해 배정될 수 있는 시간
- 훈련을 위해 이용될 수 있는 자원(직원, 공간, 사무 기구, 정보시스템과 네트워크 그리고 통신설비)의 정도
- 재정적인 한계
- 훈련으로 인해 허용될 수 있는 업무 중단의 정도

2) 모의훈련 수행

재해복구관리자는 모의훈련에 서비스거부공격, 해킹 등 전자적 침해사고에 대비한 복구 및 소집 테스트 등을 포함하여 실시한다.

- 재해복구관리자는 재해복구 모의훈련 과정의 평가를 위해 제3자 또는 외부 전문인력과 협조할 수 있다.
- 재해복구관리자는 모의훈련과정 전반에 걸쳐 다음 각 호의 사항을 포함하여 훈련을 실시한다.
    - 사건의 신고 접수 시간

- 업무 복구 목표가 성취되는 시간
- 계획의 실행 가능성에 의문을 제기하는 사건
- 제3자와의 접촉 내용과 시간
- 시험에 영향을 미치는 실제 사건의 세부적인 사항
- 시험이 종결되는 시간
- 훈련 시 실제 백업자료를 이용한 복구 가능 여부 등

3) 모의훈련 결과보고 및 사후조치

재해복구관리자는 모의훈련이 종료된 후 훈련결과에 대해 다음 각 호의 사항을 포함하는 재해복구 모의훈련 결과 보고서를 작성하여 최고경영자 및 금융감독원에 보고한다.

- 모의훈련목표 대비 달성 정도
- 모의훈련에 참여한 인원의 의견
- 모의훈련결과 도출된 문제점 및 개선방안 등

재해복구관리자는 모의훈련결과 분석에 따라 도출된 문제점 및 개선방안을 재해복구계획에 반영하여 수정하도록 해야 하며, 모의훈련결과에 따라 수정이 필요한 사항이 있는 경우에 차기 모의훈련에 반드시 포함하여 그 적정성을 검토해야 한다. 재해복구관리자는 재해나 다른 중요한 사건에 대응하는 방식을 관련 부서에 공유하고, 책임과 역할에 대해서 인식할 수 있도록 교육을 실시한다.

4) 재해복구 관리

- 유지보수 관리: 재해복구책임자는 정책의 변화, 조직구조, 인원의 변동 및 모의훈련결과 개선사항 도출 등으로 인해 'IT재해복구 운영 지침'의 보완이 필요한 경우 재•개정 관리를 한다. 또한 재해복구책임자는 장애 또는 재해가 발생하는 경우 즉시 활용이 가능하도록 'IT재해복구 운영 지침'을 연 1회 이상 검토하여 최신성을 유지한다.

- 재해복구담당자 관리: 재해복구책임자는 효과적인 'IT재해복구 운영 지침'의 유지보수를 위해 업무별 재해복구담당자를 지정한다. 관련 부서의 장은 업무별 IT재해복구담당자의 소속 부서가 변경된 경우 재해복구관리자에게 변경사항을 알린다.

- 비상연락체계 관리: 재해복구관리자는 IT재해복구의 효과적인 수행을 위해 임직원, 유관기관 및 공급업체(벤더) 등과 비상연락체계를 수립하여 운영하며, 비상사태가 발생하는 경우 비상연락망을 통하여 재해복구담당자가 즉시 대응할 수 있도록 한다. 또한 재해복구관리자는 비상사태 발생시 인원 확인 및 중요자료의 반출 등 비상 대응을 수행하기 위해 비상연락체계의 최신성을 유지한다.

**비상연락망**

# 비상연락망(장애/재해)

| 담 당 자 | 관 리 자 | 책 임 자 |
|---|---|---|
| | | |

## ㈜글로벌머니익스프레스 비상연락망

| 이름 | 부서 | 직급 | 역할 | 연락처 |
|---|---|---|---|---|
| 성종화 | 대표이사 | CEO | 최고경영자,<br>비상대책위원장 | 010-4163-7562 |
| 김한성 | IT | CISO<br>팀장 | 재해복구책임자,<br>정보보호최고책임자,<br>시스템 총괄자,<br>보안 총괄자 | 010-9216-1470 |
| 이영우 | IT | 팀원 | 재해복구관리자,<br>정보보호관리자, | 010-5210-5713 |
| 정다연 | IT | 팀원 | 재해복구담당자,<br>정보보호담당자, | 010-5114-9907 |

## KT IDC 비상연락망

| 기관명 | 이름 | 직급 | 역할 | 연락처 |
|---|---|---|---|---|
| ㈜제노솔루션 | 김상일 | 팀장 | 서버 운영,<br>사고접수 및 관리 | 010-9926-0031 |
| | 원현우 | 대리 | 서버 운영,<br>사고 분석, | 010-9949-9823 |
| | 정호중 | 사원 | 서버 운영,<br>사고 분석 | 010-6242-9675 |
| ㈜윈스 | 박택수 | 차장 | 보안관제 | 010-9770-3786 |

## 통신/보안장비 엔지니어 비상연락망

침해대응협조기관

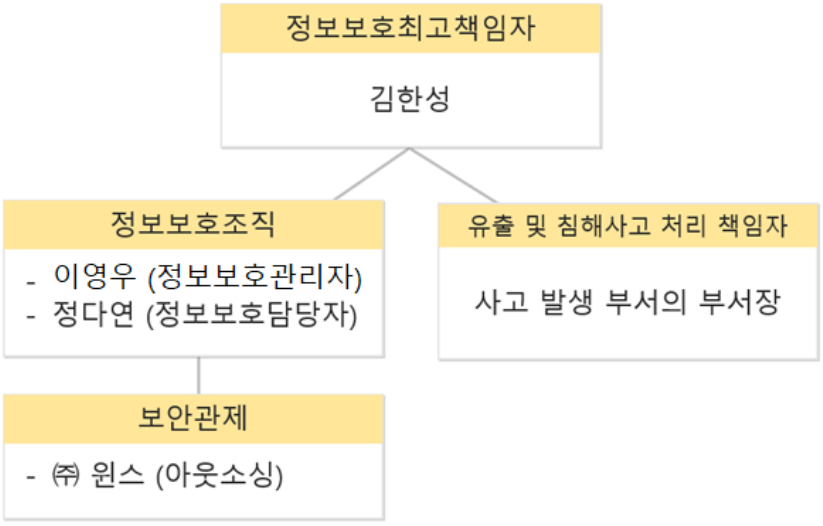
| 기 관 명 | 이름 | 직급 | 역할 | 연락처 |
|---|---|---|---|---|
| ㈜위드네트웍스 | 박동준 | 차장 | Fortigate 방화벽 | 010-3191-9171 |
| ㈜다원티에스 | 신현태 | 과장 | Genian NAC | 010-3087-5789 |
| ㈜디모아 | 김준언 | 사원 | 안랩 V3/EPP Privacy Management | 010-4920-6335 |

| 기관 | 담당 부서 | 연락처 | |
|---|---|---|---|
| | | 전화번호 | 홈페이지 및 이메일 |
| 국가정보원 | 국가사이버안전센터 | 111 | service1.nis.go.kr<br>info@ncsc.go.kr |
| 대검찰청 | 인터넷범죄수사센터 | 02-530-4949 | www.spo.go.kr<br>icic@icic.sppo.go.kr |
| 한국인터넷진흥원 | 인터넷침해사고대응지원센터 | 118 | www.krcert.or.kr<br>www.kisa.or.kr |
| 경찰청 | 사이버테러 대응센터 | 02-363-0112 | www.ctrc.go.kr |
| 한국침해사고대응팀 협의회 | 침해사고 관련 정보 및 기술 상호교환 | 02-405-5524 | www.concert.or.kr |
| 금융감독원 | 금융정보교환망시스템 | 02-3145-5440 | fines.fss.or.kr |
| 금융보안원 | 침해대응부 | 02-3495-9494 | cert@fsec.or.kr |

## 침해사고 대응

### 침해사고 대응 조직 및 역할

1) 조직도




2) 역할

| | |
|---|---|
| 정보보호최고책임자 | - 정보보호최고책임자는 개인정보 유출 및 침해사고 예방, 처리 및 재발방지의 총괄 관리 책임을 진다.<br>- 정보보호최고책임자는 개인정보 유출 및 침해사고 발생시 처리책임자를 지정하고 대응팀을 소집하여 운영한다. |
| 정보보호조직<br>(침해사고 대응팀) | - 개인정보보호책임자가 해당 개인정보 유출 및 침해사고 분석, 대응 및 복구에 필요한 관련자를 지정하여 소집한다. |
| 유출 및 침해사고 처리 책임자 | - 해당 개인정보 유출 및 침해사고 발생 부서의 부서장으로 지정되며, 처리 및 재발방지에 대한 책임을 지고 정보보호조직과 협력하여 사고를 해결한다. |
| 정보보호 관리자 | - 개인정보 유출 및 침해사고를 접수하고, 등급을 분류하여 침해사고 대응 절차를 개시한다.<br>- 정보보호조직(침해사고 대응 팀)의 간사로서 대내외 비상연락망을 관리하고 팀 내 연락 및 조정을 담당한다.<br>- 개인정보 유출 및 침해기록을 관리하고 필요시 관련자 및 기관에 보고한다.<br>- 필요 시 정보보안에 대한 기술적인 분석을 담당한다. |
| 전 직원 | - 개인정보 유출 및 침해가 발생한 것을 인지한 경우, 지체없이 정보보호최고책임자에게 신고해야 한다. |

**침해사고 등급 분류**

| 침해등급 | 내용 |
|---|---|
| 1 등급<br>(긴급) | - 서비스 거부공격(DDoS), 바이러스 등으로 인한 전체 서비스가 중단되는 경우<br>- 기밀정보를 보유한 시스템의 해킹으로 인한 정보의 유출<br>- 전사적 차원에서 공동 대처해야 할 필요성이 있는 경우 |

| | |
|---|---|
| 2 등급<br>(주의) | - 외부 또는 내부로부터의 계속적인 불법적 접근시도가 발견되는 경우<br>- 외부 또는 내부로부터의 비정상적 패킷들의 전송량이 증가하는 경우<br>- 확산속도가 빠른 바이러스가 외부에서 발생한 경우 |
| 3 등급<br>(관심) | - 대/내외 서비스에 영향을 주지 않는 바이러스, 비정상 traffic 발견 시<br>- 기타 회사에 직접적인 영향이나 이미지 손상이 없으나, 타사 등 외부에서 피해사례가 보고되는 경우 |

**침해사고 신고**

본사의 직원이 취급하는 개인정보에 대해서 개인정보유출 및 침해가 발생한 것을 인지한 경우 또는 그런 침해의 발생이 의심되는 경우 지체없이 정보보호담당자에게 알린 후, 개인정보침해 업무를 담당하는 정부기관에 신고해야 한다.

**침해사고 조사**

1) 침해사고 신고접수

① 회사 전 임직원은 정보보호 침해사고의 징후가 있거나 침해사고의 발생을 인지한 때 즉시 침해사고대응팀에 신고하여야 한다.

② 침해사고 최초 발견자는 사고 피해를 최소화하기 위해 선 조치가 필요하다고 판단한 경우 적절한 대응 조치를 취한 후 보고한다.

③ 침해사고 최초 발견자는 사고를 은폐하거나 축소하기 위한 행동을 해서는 안된다.

④ 침해사고대응팀장은 정보보호사고 신고 접수 시 침해사고 대응 절차에 의거하여 사고 개요를 작성하고, 정보보호최고책임자에게 보고하여야 한다.

2) 침해사고 처리 및 분석

① 침해사고 대응 팀은 발생된 침해사고에 대하여 지체 없이 원인조사, 분석, 증거 확보 및 대응조치 등이 수행하여야 한다. 조사 및 처리를 위해 전문인력이 필요할 경우 타부서나 외부 전문가의 도움을 받을 수 있다.

② 침해사고의 형태, 조사결과, 피해정도 등을 종합하여 중대한 사고에 해당할 경우 정보보호위원회를 긴급 소집하여 위원장(정보보호최고책임자)의 주관 하에 공동 대응책을 논의할 수 있다.

① 정보보호 사고 원인을 조사하고 응급조치가 취해진 후 그 결과는 정보보호 최고책임자에게 보고되어야 한다.
④ 정보보호 사고 내용에 대하여 세부 원인 및 경위에 대한 조사가 종결될 때까지는 공개하지 않는다.

⑤ 사이버 침해사고 분석 시 고려하여야 할 사항은 아래의 각 호와 같다.

- 사고 발생 원인분석: 공격자가 시스템에 어떻게 침입했는지에 대해서 분석한다. 주로 특정 어플리케이션의 취약성, 시스템의 잘못된 설정, 계정도용 등을 이용하여 침입한다.

- 사고의 발생 시간: 공격자가 언제 처음으로 시스템에 침입했는지 분석하고, 최초 침입 이후 재침입이 있었는지 등에 대해서 분석한다.
- 사고 발생 범위: 하나의 시스템이 공격당했을 시, 다른 시스템도 공격을 당했을 가능성이 많으므로 반드시 피해여부를 확인한다.
- 공격자 출처: 공격자의 IP 주소를 찾아내고 해당 IP 를 사용하는 기관 정보를 분석한다.
- 공격 목적: 공격자가 피해시스템에서 어떠한 활동을 했는지 분석하여 공격 목적을 확인한다. 주로 정보유출, 단순한 침입, 공격시스템으로 사용하기 위한 목적 등이 있을 수 있다.
- 분석과정 기록: 침해사고 분석과정과 분석 로그, 흔적들은 기록되고 보존되어야 한다.

  가. 분석방법 및 내용, 분석시간, 분석 이유 등

  나. 시스템 로그, 침입차단 및 탐지시스템 등의 정보보호시스템 로그

  다. 피해시스템에서 발견된 파일 등

  라. 공격의 흔적들이 기록된 파일들은 훼손되지 않아야 한다.

3) 침해사고 복구

침해사고 복구 단계에서는 취약성 제거, 피해시스템 복구, 관련자 통지, 보안대책 구현 등의 작업을 수행한다.

- 취약성 제거: 공격에 이용된 취약성을 제거하여야 한다. 시스템 뿐 아니라 피해시스템과 유사한 종류의 시스템에 대해서 모두 분석하고 같은 취약성이 발견되면 이를 제거한다.
- 피해 시스템 복구: 취약성 제거를 한 다음 정상적인 서비스가 이루어지도록 시스템을 복구한다. 만약 취약성 제거와 분석이 완벽하게 이루어지지 않았다고 판단되면, 시스템을 다시 설치하고 최신 백업 버전으로 복구한다.
- 관련자 통지: 사고와 관련된 모든 이해 관계자에게 분석결과를 통지하여야 하며, 사고와의 관련성에 따라 통지하는 정보의 정도가 달라야 한다. 외부기관에 제공하는 정보는 사이트 내의 민감한 정보는 포함되지 않아야 하며, 상대가 필요로 하는 정보만을 전달하도록 한다.

**침해사고 보고 및 사후 조치**

1) 결과 보고

- 사고와 관련된 모든 로그파일과 분석기록 침입 흔적들은 안전하게 저장하여 보관하여야 한다.
- 침해사고 분석 및 대응이 종료되면 사고 처리 결과에 대한 '침해사고 처리결과 보고서'를 작성한다.
- 보고서 내용은 사고분석 및 대응 과정의 모든 내용과 비슷한 유형의 사고 방지를 위한 개선방향 등이 포함되도록 작성하고 정보보호최고책임자에게 보고한다.

2) 재발방지 및 모의훈련

- 침해사고대응팀은 침해사고로 인해 제2, 제3의 피해를 막고 재발을 방지하기 위해 아래의 활동을 수행한다.
    - 조직 및 정보자산의 위험 및 우선순위를 재식별하고 기존 보호대책을 재검토한다.
    - 재발 및 유사 사고를 예방하고 탐지하기 위한 관리적, 기술적, 물리적 후속 조치를 수행한다.
    - 정보보호관리자는 침해사고에 대한 관련자들의 공유 및 재발 방지를 위한 교육활동을 계획하여 이행한다.
    - 침해사고대응팀장은 침해사고 원인 및 처리결과 등을 금융감독원, 금융분야 침해사고대응기관(금융보안원), 한국인터넷진흥원, 등 관련 기관과 정보공유를 통해 유사사고 재발방지 대책을 강구하여야 한다.
- 침해사고의 원인이 직원의 과실에 의해 사고가 발생한 경우 내부 규정에 따라 필요한 징계 절차가 수행되어야 한다.
- 사고분석 결과로 인한 개선사항이 보안정책 및 대책에 반영되어야 한다.
- 정보보호 최고책임자는 자체 정보통신망 또는 시스템을 대상으로 매년 1회 이상 또는 수시 사이버위기 대응 모의훈련 계획을 수립하여 실시하고 결과보고서를 작성하여 금융분야 침해대응기관(금융보안원)에 보고하여야 한다.

3) 사고상황 전파

- 정보보호최고책임자는 사이버공격과 관련한 정보를 확인한 경우에는 전화·팩스·이메일 등 통신수단을 활용하여 그 사실을 금융감독원, 금융분야 침해사고대응기관, 한국인터넷진흥원 등 관계기관에 통보한다.
- 제1항에 따라 통보해야 할 사항은 다음 각 호와 같다.
    - 사이버공격으로 인하여 피해가 발생하거나 피해 발생이 예상되는 경우
    - 사이버공격이 확산될 우려가 있는 경우
    - 그 밖에 사이버공격 계획 등 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우

4) 정보보안 사고 조사

- 정보보호최고책임자는 침해사고가 발생한 때에 즉시 피해확산 방지를 위한 조치를 취하여야 한다. 이 경우, 사고원인 규명 시까지 피해 시스템에 대한 증거를 보전하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니된다.

- 일시 및 장소
- 사고 원인, 피해현황 등 개요
- 사고자 및 관계자의 인적사항
- 조치내용 등

정보보호 최고책임자는 관련자 징계, 재발방지를 위한 보안대책의 수립·시행 등 사고 조사 결과에 따른 필요한 조치를 취하여야 한다.

**비상연락망**

# 비상연락망(침해사고)

| 담 당 자 | 관 리 자 | 책 임 자 |
|---|---|---|
| | | |

**㈜글로벌머니익스프레스 비상연락망**

| 이름 | 부서 | 직급 | 역할 | 연락처 |
|---|---|---|---|---|
| 성종화 | 대표이사 | CEO | 최고경영자 | 010-4163-7562 |
| 김한성 | IT | CISO<br>팀장 | 정보보호최고책임자<br>시스템 총괄자<br>보안 총괄자 | 010-9216-1470 |
| 이영우 | IT | 팀원 | 정보보호관리자 | 010-5210-5713 |
| 정다연 | IT | 팀원 | 정보보호담당자 | 010-5114-9907 |

**KT IDC 비상연락망**

| 기관명 | 이름 | 직급 | 역할 | 연락처 |
|---|---|---|---|---|
| ㈜제노솔루션 | 김상일 | 팀장 | 서버 운영,<br>사고접수 및 관리 | 010-9926-0031 |
| | 원현우 | 대리 | 서버 운영,<br>사고 분석, | 010-9949-9823 |
| | 정호중 | 사원 | 서버 운영, | 010-6242-9675 |

| | | | | |
|---|---|---|---|---|
| | | | 사고 분석 | |
| ㈜윈스 | 박택수 | 차장 | 보안관제 | 010-9770-3786 |

## 통신/보안장비 엔지니어 비상연락망

| 기 관 명 | 이름 | 직급 | 역할 | 연락처 |
|---|---|---|---|---|
| ㈜위드네트웍스 | 박동준 | 차장 | Fortigate 방화벽 | 010-3191-9171 |
| ㈜다원티에스 | 신현태 | 과장 | Genian NAC | 010-3087-5789 |
| ㈜디모아 | 김준언 | 사원 | 안랩 V3/EPP Privacy Management | 010-4920-6335 |

**침해대응협조기관**

| 기관 | 담당 부서 | 연락처 | |
|---|---|---|---|
| | | 전화번호 | 홈페이지 및 이메일 |
| 국가정보원 | 국가사이버안전센터 | 111 | service1.nis.go.kr<br>info@ncsc.go.kr |
| 대검찰청 | 인터넷범죄수사센터 | 02-530-4949 | www.spo.go.kr<br>icic@icic.sppo.go.kr |
| 한국인터넷진흥원 | 인터넷침해사고대응지원센터 | 118 | www.krcert.or.kr<br>www.kisa.or.kr |
| 경찰청 | 사이버테러 대응센터 | 02-363-0112 | www.ctrc.go.kr |
| 한국침해사고대응팀 협의회 | 침해사고 관련 정보 및 기술 상호교환 | 02-405-5524 | www.concert.or.kr |
| 금융감독원 | 금융정보교환망시스템 | 02-3145-5440 | fines.fss.or.kr |
| 금융보안원 | 침해대응부 | 02-3495-9494 | cert@fsec.or.kr |