**[10] 물적 시설설비 현황**

[10] 물적시설설비현황 목차

[**10-1. 전산기기 보유 현황** 6](#_Toc80635718)

[**1-1. 전산기기 목록** 6](#_Toc80635719)

[**1-1-1. KT IDC 랙 실장도** 6](#_Toc80635720)

[**1-1-2. KT IDC 하드웨어** 6](#_Toc80635721)

[**1-1-3. KT IDC 서버 VM 목록** 7](#_Toc80635722)

[**1-1-4. KT IDC 통신기기 목록** 7](#_Toc80635723)

[**1-1-5. 본사 랙 실장도** 9](#_Toc80635724)

[**1-1-6. 본사 통신기기 목록** 10](#_Toc80635725)

[**10-2. 백업장치 구비 현황** 12](#_Toc80635726)

[**2-1. 백업계획서** 12](#_Toc80635727)

[**2-1-1. 백업목적** 12](#_Toc80635728)

[**2-1-2. 백업 조직도** 12](#_Toc80635729)

[**2-1-3. 백업 수행 절차** 12](#_Toc80635730)

[**2-1-4. 백업 대상 및 범위** 13](#_Toc80635731)

[**2-1-5. 백업 및 소산 방법** 13](#_Toc80635732)

[**2-1-6. 백업 보관 정책** 13](#_Toc80635733)

[**2-1-7. 백업 관리 양식** 14](#_Toc80635734)

[**2-2. 비상계획서** 19](#_Toc80635735)

[**2-2-1. 비상 계획 목적** 19](#_Toc80635736)

[**2-2-2. 재해 복구 조직 및 역할** 19](#_Toc80635737)

[**2-2-3. 비상 상황 구분** 21](#_Toc80635738)

[**2-2-4. 재해 복구** 22](#_Toc80635739)

[**2-2-5. 재해해제 및 후속조치** 23](#_Toc80635740)

[**2-2-6. 모의 훈련** 24](#_Toc80635741)

[**2-2-7. 비상연락망** 26](#_Toc80635742)

[**2-3. 침해사고 대응** 28](#_Toc80635743)

[**2-3-1. 침해사고 대응 조직 및 역할** 28](#_Toc80635744)

[**2-3-2. 침해사고 등급 분류** 30](#_Toc80635745)

[**2-3-3. 침해사고 신고** 30](#_Toc80635746)

[**2-3-4. 침해사고 조사** 30](#_Toc80635747)

[**2-3-5. 침해사고 보고 및 사후 조치** 32](#_Toc80635748)

[**2-3-6. 비상연락망** 34](#_Toc80635749)

[**2-4. 주요 전산장비, 통신회선 등의 이중화 구성도** 36](#_Toc80635750)

[**3. 각종 프로그램 보유 현황** 37](#_Toc80635751)

[**3-1. 프로그램 보유 현황** 37](#_Toc80635752)

[**3-1-1. 프로그램 정의 및 목적** 37](#_Toc80635753)

[**3-1-2. 프로그램 설명서** 37](#_Toc80635754)

[**3-1-3. 보유 프로그램 및 DB 목록** 43](#_Toc80635755)

[**3-2. 프로그램 등록, 변경, 폐기 절차** 46](#_Toc80635756)

[**3-2-1. 변경요청** 46](#_Toc80635757)

[**3-2-2. 변경 수행 및 통제** 46](#_Toc80635758)

[**3-2-3. 응용 프로그램 폐기** 50](#_Toc80635759)

[**3-2-4. 프로그램 관리 양식** 50](#_Toc80635760)

[**10-4. 정보처리시스템 관리방안** 52](#_Toc80635761)

[**4-1. 계정 및 비밀번호 부여절차** 52](#_Toc80635762)

[**4-1-1. 계정 관리 양식** 54](#_Toc80635763)

[**4-2. 접근 권한 통제** 56](#_Toc80635764)

[**4-3. 전산자료 반출입 통제** 59](#_Toc80635765)

[**4-3-1. 전산자료 관리 양식** 60](#_Toc80635766)

[**4-4. 전산 개발 규정** 62](#_Toc80635767)

[**4-4-1. 개발/테스트/운영 환경 및 업무 분리** 62](#_Toc80635768)

[**4-4-2. 보안 요구사항 분석 및 개발** 63](#_Toc80635769)

[**4-4-3. 응용프로그램 테스트 및 테스트 데이터 통제** 63](#_Toc80635770)

[**4-4-4. 응용 프로그램 이관** 64](#_Toc80635771)

[**4-5. 접근기록 자동관리** 64](#_Toc80635772)

[**4-5-1. 중요정보 조회 시** 64](#_Toc80635773)

[**4-5-2. 중요정보 수정 시** 65](#_Toc80635774)

[**4-6. 공개용 웹서버 보호** 66](#_Toc80635775)

[**4-7. 공개용 웹서버 계정 부여 현황** 67](#_Toc80635776)

[**4-8. 개인정보 유출 방지** 67](#_Toc80635777)

[**4-8-1. 개인정보 보유현황** 67](#_Toc80635778)

[**4-8-2. 개인정보 유출 방지** 68](#_Toc80635779)

[**4-9. 취약점 점검** 69](#_Toc80635780)

[**4-9-1. 점검 목적** 69](#_Toc80635781)

[**4-9-2. 점검 대상 및 주기** 69](#_Toc80635782)

[**4-9-4. 점검 항목** 71](#_Toc80635783)

[**10-5. 감시운영체제 구축 현황** 72](#_Toc80635784)

[**5-1. 정보보호시스템 구축 현황** 72](#_Toc80635785)

[**5-1-1. KT IDC 정보보호시스템 구축 현황** 72](#_Toc80635786)

[**5-1-2. 본사 정보보호시스템 구축 현황** 73](#_Toc80635787)

[**5-2. 망분리 현황** 75](#_Toc80635788)

[**5-3. 악성코드 감염 방지대책** 77](#_Toc80635789)

[**10-6. 전산실 안정성 확보 및 보안대책** 79](#_Toc80635790)

[**6-1. 전산실 설비 목록** 79](#_Toc80635791)

[**6-2. 비상대책** 79](#_Toc80635792)

[**6-3. 보호구역 지정 현황** 80](#_Toc80635793)

[**6-4. 전산실 출입자 관리 기록** 80](#_Toc80635794)

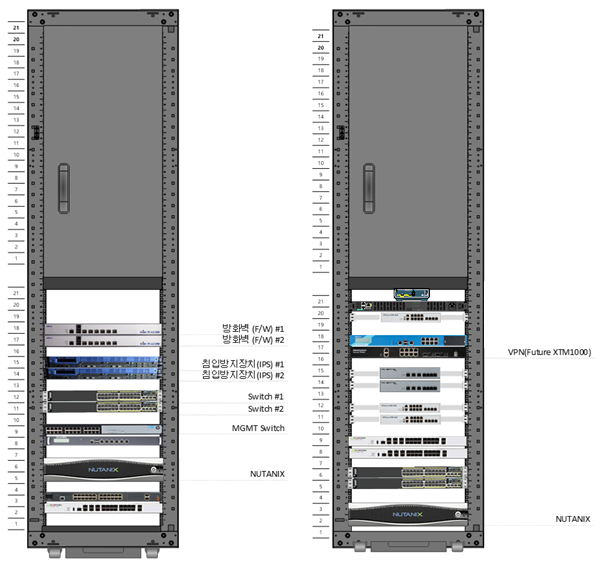
[**6-5. 출입자 감시장치 운영현황** 82](#_Toc80635795)

[**6-6. 전산실 배치도** 82](#_Toc80635796)

# **10-1. 전산기기 보유 현황**

## **1-1. 전산기기 목록**

### **1-1-1. KT IDC 랙 실장도**



### **1-1-2. KT IDC 하드웨어**

|  |  |  |  |
| --- | --- | --- | --- |
| 모델명 | 서버명 | 사양 | 기능 |
| Nutanix | NX-1065S-G5 | CPU 40vCore  Memory 96GB  SSD 480GB  HDD 4TB | 가상화 서버 |
| Nutanix | NX-1065S-G5 | CPU 40vCore  Memory 128GB  SSD 480GB  HDD 4TB | 가상화 서버 |

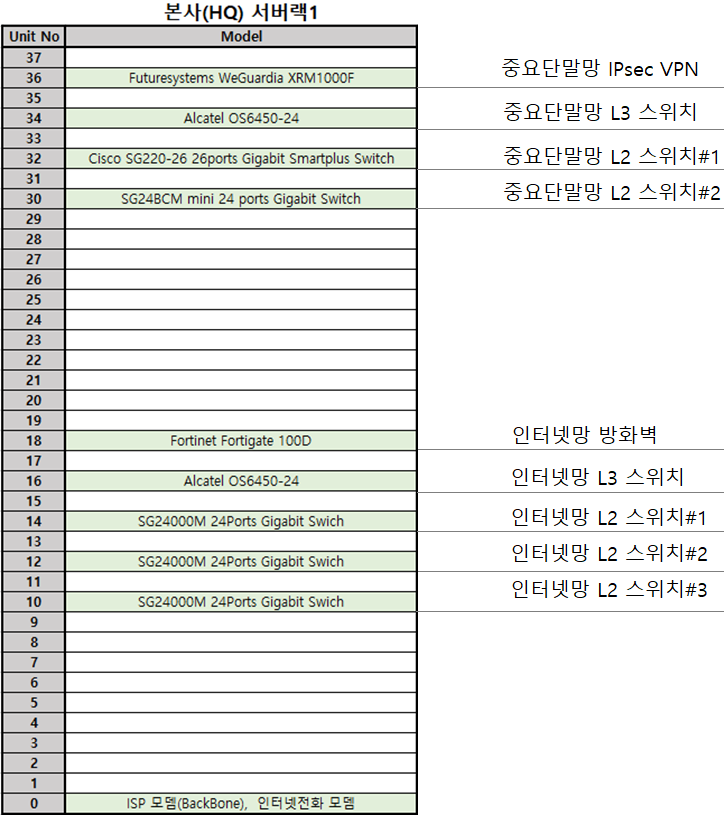
### **1-1-3. KT IDC 서버 VM 목록**

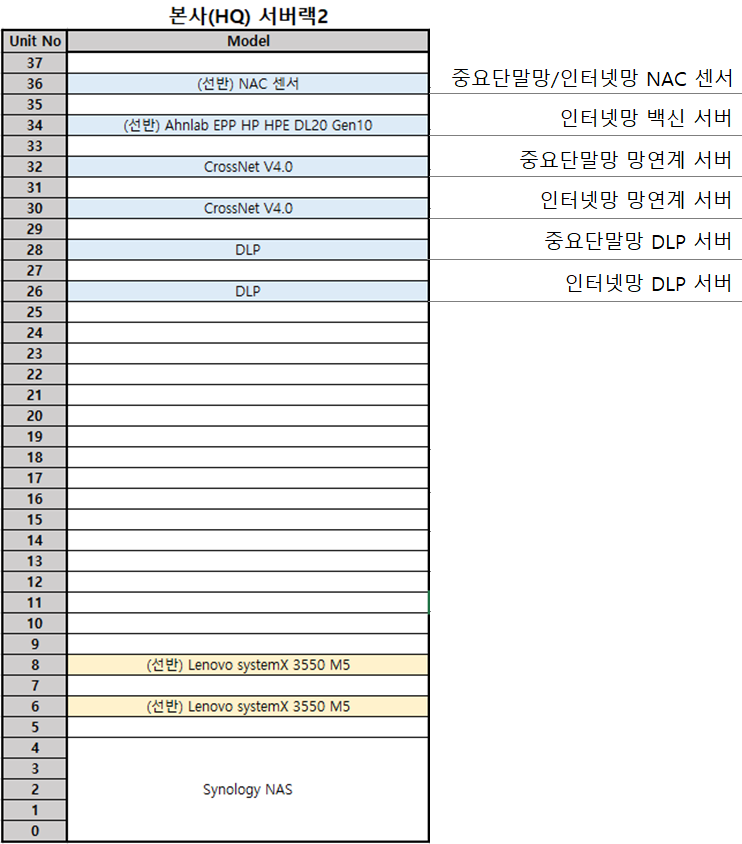
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 위치 | 구분 | Server | Internal IP | description |
| 내부 | DB | PROD-DB-001 | 10.25.10.151 | 운영 DB Server (1호기) |
| PROD-DB-002 | 10.25.10.152 | 운영 DB Server (2호기) |
| 내부 | DEV | UAT-DB-01 | 10.25.12.100 | 개발 DB Server |
| STAG-DB-01 | 10.25.10.60 | 테스트 DB Server |
| SVN-SVR-01 | 10.25.12.200 | 형상관리 서버 |
| 내부 | 업무시스템 | PROD-CORE-02 | 10.25.12.250 | 운영 관리자 페이지 |

### **1-1-4. KT IDC 통신기기 목록**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 구분 | 벤더 | 모델명 | 제원 | 수량 | 기능 |
| F/W | Wins | Sniper  AP2000 | CPU 2Core 3.5GHz  Memory 4GB  HDD 1TB  CF Memory 4GB  NIC 1GF \* 4port, 1GC \* 8port  Power Dual  Throughput 6Gbps | 2 | 방화벽(이중화) |
| IPS | Wins | Sniper  One-I 1000 | CPU 4Core 3.5GHz  Memory 32GB  HDD 2TB  CF Memory 4GB  NIC 1GF \* 2port, 1GC \* 4port  Power Dual  Throughput 4Gbps | 2 | 침입방지시스템  (이중화) |
| Switch | Cisco | C2960XR | CPU 2Core 600MHz  Memory 512MB  Flash Memory 128MB  NIC 1G \* 24port  Power Dual | 2 | L2 스위치  (이중화) |
| Management  Switch | HP | 1410-24-R | NIC 100M \* 24port  Power Single  Throughput 3.5Mpps  Switch capacity 4.8Gbps | 1 | 관리 스위치 |
| VPN | FutureSystems | XTM1000F | CPU 2Core 700MHz Memory 1GB HDD N/A CF Memory 4GB NIC 1G \* 8port Concurrent Session 500,000 CPS 15,000 Power Single | 1 | KT IDC-HQ(본사) 중요단말망 연결용 IPsec VPN (방화벽 기능 포함) |

### **1-1-5. 본사 랙 실장도**





### **1-1-6. 본사 통신기기 목록**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 구분 | 벤더 | 모델명 | 제원 | 수량 | 기능 |
| IPsec VPN | FutureSystems | XTM1000F | CPU 2Core 700MHz Memory 1GB HDD N/A CF Memory 4GB NIC 1G \* 8port Concurrent Session 500,000 CPS 15,000 Power Single | 1 | KT IDC-HQ(본사) 중요단말망 연결용 IPsec VPN(방화벽 기능 포함) |
| F/W | Fortinet | Fortigate 100D | CPU 4Core  Memory 3.8GB  HDD 32GB  Latency 37 ms | 1 | 인터넷망 방화벽 |
| L3 Switch | Alcatel | Alcatel OS6450-24 | 24ports  10 GigE | 2 | 중요단말망, 인터넷망 L3 스위치 |
| L2 Switch | ipTime | SG24BCM mini | 24ports  48Gbps | 1 | 중요단말망  L2 스위치 |
| L2 Switch | Cisco | SG220-26 | 26 ports  52Gdps | 1 | 중요단말망  L2 스위치 |
| L2 Switch | ipTime | SG24000M | 24ports  1000Mbps | 3 | 인터넷망  L2 스위치 |

# **10-2. 백업장치 구비 현황**

## **2-1. 백업계획서**

### **2-1-1. 백업목적**

정보시스템의 장애, 화재와 같은 재해 또는 해킹으로 인한 정보의 망실에 대비하여 파일 또는 데이터베이스를 복사해 별도의 매체에 저장 및 관리하기 위함이다.

### **2-1-2. 백업 조직도**



### **2-1-3. 백업 수행 절차**

**텍스트, 시계이(가) 표시된 사진

자동 생성된 설명**

|  |  |  |  |
| --- | --- | --- | --- |
| 순서 | 수행절차 | 수행자 | 양식 |
| 1 | 신규요청  - 신규 대상시스템에 대해서 백업요청 | 업무 담당자 | 백업 신청서 |
| 2 | 백업요청서 검토 및 승인 | 업무 팀장 |  |
| 3 | 업무부서는 백업요청서를 백업운영 부서에 이행 요청  백업운영자는 백업요청 접수 처리 | 백업운영자 | 백업 신청서 |
| 4 | 백업 요청 내역에 대한 타당성 분석 및 백업 이행 승인  백업 운영자에 작업 이행 지시 | 백업운영팀장 |  |
| 5 | 백업 운영자는 작업요청 계획에 따라 작업 이행  백업 이력관리 대장 작성 | 백업운영자 | 백업이력 관리대장 |

### **2-1-4. 백업 대상 및 범위**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 대상 | 범위 | 방식 | 주기 | 매체 | 소산 주기 |
| 시스템 백업(OS) | OS 파일 시스템 백업(Boot 영역) | Full (Nutanix 서버 스냅샷) | 매일 | 스토리지 | 매일 |
| 데이터 베이스 | SQL 프로그램 | Full (Nutanix 서버 스냅샷) | 매일 | 스토리지 | 매일 |
| 운영 데이터/구성파일 | DB 작업 스케줄러 | 매일 | 스토리지 | 매일 |
| DB Log | DB 작업 스케줄러 | 매일 | 스토리지 | 매일 |
| 파일 시스템 백업 | Application 실행 파일 및 소스 |  | - 백업 요청에 의한 월1회 백업 (단, 개발 소스의 경우 운영 별도 분리보관 정책 반영) | 스토리지 | 월 1회 |

### **2-1-5. 백업 및 소산 방법**

|  |  |
| --- | --- |
| 구분 | 보호대책 내역 |
| DB작업 스케줄러에 의해 자동 백업된 데이터베이스 운영 데이터/구성파일, DB log | * 본사 내화금고 내 소산보관을 위해 물리적으로 외장하드 보관 및 보호, 화재 시 데이터 파손 방지 및 도난 방지 * 내부 출입통제 및 감시설비를 통한 모니터링 * 소산 시 담당자 및 운영자 통제를 위한 출입/작업 이력관리 |

### **2-1-6. 백업 보관 정책**

모든 전자금융거래기록을 거래금액의 크기와 관련 없이 5년간 보관한다.

### **2-1-7. 백업 관리 양식**

백업 관리를 위해, 다음의 양식을 통해 데이터 백업, 소산, 복구 현황과 백업 매체를 관리한다.

[별지1] 백업관리대장 작성예

테이블이(가) 표시된 사진

자동 생성된 설명

[별지2] 소산관리대장 작성예

테이블이(가) 표시된 사진

자동 생성된 설명

[별지3] 백업매체관리대장 작성예

테이블이(가) 표시된 사진

자동 생성된 설명

[별지4] 백업소〮산신청서 작성예

테이블이(가) 표시된 사진

자동 생성된 설명

[별지5] 복구신청서 작성예

테이블이(가) 표시된 사진

자동 생성된 설명

## **2-2. 비상계획서**

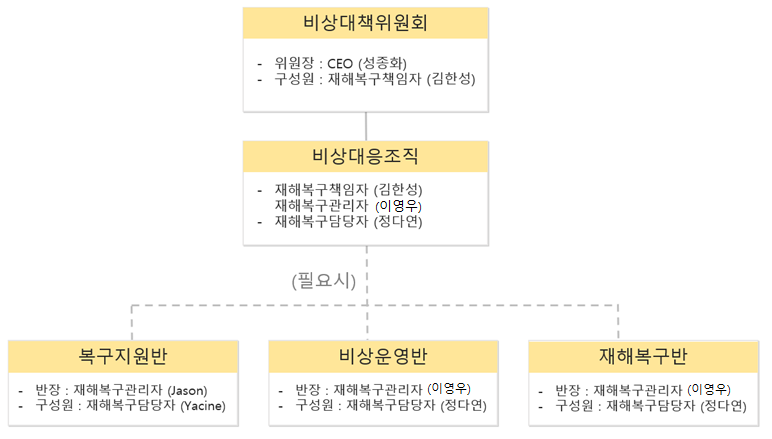
### **2-2-1. 비상 계획 목적**

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 IT서비스를 제공할 수 없는 상태를 말한다.
2. ‘재해’는 자연적, 인위적 재난 또는 위해로 인하여 IDC, 서버실 및 장비실의 정보시스템을 가동할 수 없거나 IT관련 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.

### **2-2-2. 재해 복구 조직 및 역할**

1) 조직도



1. 역할
2. 비상대책위원장은 상황Ⅲ, 상황Ⅳ 및 상황Ⅴ 이외에도 중대한 비상사태라고 판단되는 경우 비상대책위원회를 소집할 수 있다.
3. 비상대책위원장은 상황Ⅲ, 상황Ⅳ 및 상황Ⅴ의 경우 재해를 선포하고 대체장소로의 이동을 결정한다.
4. 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  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  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 | IT인프라의 복구와 관련한 역할을 담당 | 반장: 재해복구관리자  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. |

1. 재해복구 정책
2. 재해복구책임자는 재해복구 전략, 비상대응조직 역할, 보고체계, 비상사태별 대응 및 복구계획, 모의훈련계획, 유지보수계획, 비상연락체계 등의 재해복구 정책을 수립한다.
3. 재해복구책임자는 재해복구 정책 및 전략의 실효성을 검토하기 위해 연 1회 비상대응 모의훈련계획을 수립해야 한다.
4. 재해복구책임자는 경영환경 변화 및 조직구조 개편 등 주요 변동사항이 발생할 경우 복구목표시간, 복구시점 및 복구우선순위를 검토하여 변경사항을 재해복구 정책에 반영한다.
5. 재해복구책임자는 ‘업무영향분석(BIA, Business Impact Analysis)’을 통해 복구목표시간(RTO, Recovery Time Objective) 및 복구시점(RPO, Recovery Point Objective)을 정의한다.
6. 재해복구관리자는 핵심업무에 대해 정상적인 업무수행을 할 수 없는 경우를 대비해 대체수행자를 지정하여 운영한다.
7. 재해복구관리자는 장애 또는 재해 발생으로 인하여 업무중단이 발생하는 경우를 대비해 각 업무별 피해규모 및 업무중요도를 분석하여 최소 복구목표시간, 복구시점 및 복구우선순위를 산정한다.
8. 재해복구관리자는 복구목표시간, 복구시점 및 복구우선순위를 ‘정보시스템 복구우선순위’에 작성하여 관리한다.

1. 비상대응조직 체계
2. 재해복구책임자는 상황I, 상황Ⅱ인 경우 비상대책위원회의 소집을 요청할 수 있다.
3. 비상대책위원장은 상황Ⅲ, 상황Ⅳ, 및 상황Ⅴ인 경우 비상대책위원회를 소집한다.
4. 재해복구책임자는 비상사태가 발생하는 경우 정보시스템의 비상대응조치 및 업무처리 등을 위해 ‘복구지원반’, ‘비상운영반’ 및 ‘재해복구반(이하 ‘비상대응조직등’이라 한다)’을 운영할 수 있다.
5. 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

### **2-2-3. 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)

### **2-2-4. 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. * 운영담당자는 백업 소산장소로부터 인계 받은 백업 자료를 정보시스템 및 데이터 복구 절차에 따라 복구해야 한다. * 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. * 네트워크담당자는 기본적으로 네트워크 연결을 위한 네트워크 장비를 미리 확보해 재난에 대비한다. |

1. 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

1. 재해복구 절차
2. 신규 가상화 서버 수급
3. 소산 백업된 외장하드를 가지고 이동
4. 신규 가상화 서버에 VM 설치
5. OS 설치
6. 네트워크 설정
7. 기능 및 프로그램(MSSQL, SSMS, 닷넷, IIS) 설치
8. 소산 백업된 데이터를 신규 장비에 복원
9. 소산 백업된 앱/웹 퍼블리싱

### **2-2-5. 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.

### **2-2-6. 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

1. 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

1. 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.

1. 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 중요 자료의 반출 등 비상 대응을 수행하기 위해 비상연락체계의 최신성을 유지한다.

### **2-2-7. 비상연락망**

**비상연락망(장애/재해)**

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

**㈜글로벌머니익스프레스 비상연락망**

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

**KT IDC 비상연락망**

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

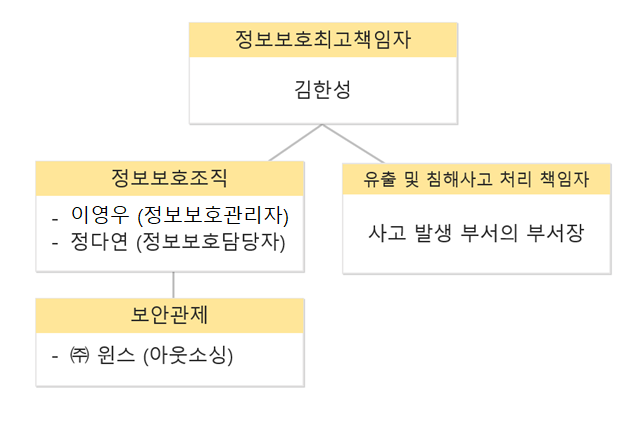
**침해대응 협조 기관**

|  |  |  |  |
| --- | --- | --- | --- |
| **기관** | **담당 부서** | **연락처** | |
| **전화번호** | **홈페이지 및 이메일** |
| 국가정보원 | 국가사이버안전센터 | 111 | service1.nis.go.kr  info@ncsc.go.kr |
| 대검찰청 | 인터넷범죄수사센터 | 02-530-4949 | www.spo.go.kr  icic@icic.sppo.go.kr |
| 한국인터넷진흥원 | 인터넷침해사고대응지원센터 | 118 | www.krcert.or.kr  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 |

## **2-3. 침해사고 대응**

### **2-3-1. 침해사고 대응 조직 및 역할**

1. 조직도



1. 역할

|  |  |
| --- | --- |
| 정보보호최고책임자 | * 정보보호최고책임자는 개인정보 유출 및 침해사고 예방, 처리 및 재발방지의 총괄 관리 책임을 진다. * 정보보호최고책임자는 개인정보 유출 및 침해사고 발생시 처리책임자를 지정하고 대응팀을 소집하여 운영한다. |
| 정보보호조직  (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. * 정보보호조직(침해사고 대응 팀)의 간사로서 대내외 비상연락망을 관리하고 팀 내 연락 및 조정을 담당한다. * 개인정보 유출 및 침해기록을 관리하고 필요시 관련자 및 기관에 보고한다. * 필요 시 정보보안에 대한 기술적인 분석을 담당한다. |
| 전 직원 | * 개인정보 유출 및 침해가 발생한 것을 인지한 경우, 지체없이 정보보호최고책임자에게 신고해야 한다. |

### **2-3-2. 침해사고 등급 분류**

|  |  |
| --- | --- |
| 침해등급 | 내용 |
| 1등급  (긴급) | - 서비스 거부공격(DDoS), 바이러스 등으로 인한 전체 서비스가 중단되는 경우  - 기밀정보를 보유한 시스템의 해킹으로 인한 정보의 유출  - 전사적 차원에서 공동 대처해야 할 필요성이 있는 경우 |
| 2등급  (주의) | - 외부 또는 내부로부터의 계속적인 불법적 접근시도가 발견되는 경우  - 외부 또는 내부로부터의 비정상적 패킷들의 전송량이 증가하는 경우  - 확산속도가 빠른 바이러스가 외부에서 발생한 경우 |
| 3등급  (관심) | - 대/내외 서비스에 영향을 주지 않는 바이러스, 비정상 traffic 발견 시  - 기타 회사에 직접적인 영향이나 이미지 손상이 없으나, 타사 등 외부에서 피해사례가 보고되는 경우 |

### **2-3-3. 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.

### **2-3-4. 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.

1. 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 IP주소를 찾아내고 해당 IP를 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.

1. 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.

### **2-3-5. 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.

1. 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.

1. 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

1. 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.

### **2-3-6. 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  팀장 | 정보보호최고책임자  시스템 총괄자  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,  사고접수 및 관리 | 010-9926-0031 |
| 원현우 | 대리 | 서버 운영,  사고 분석, | 010-9949-9823 |
| 정호중 | 사원 | 서버 운영,  사고 분석 | 010-6242-9675 |
| ㈜윈스 | 박택수 | 차장 | 보안관제 | 010-9770-3786 |

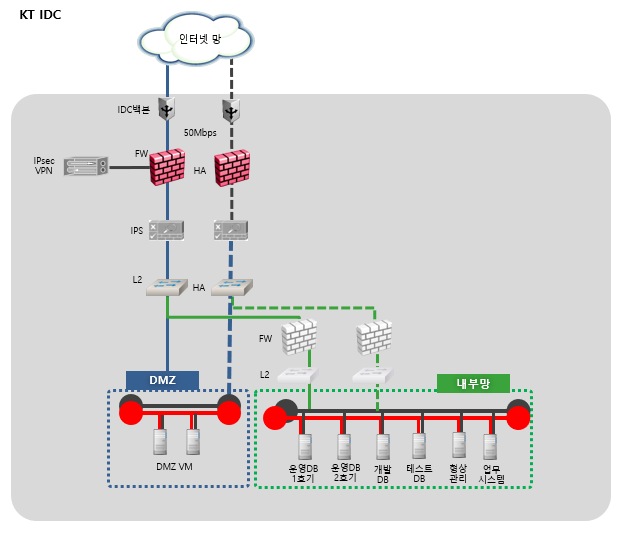
**통신/보안장비 엔지니어 비상연락망**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 |

**침해대응 협조 기관**

|  |  |  |  |
| --- | --- | --- | --- |
| **기관** | **담당 부서** | **연락처** | |
| **전화번호** | **홈페이지 및 이메일** |
| 국가정보원 | 국가사이버안전센터 | 111 | service1.nis.go.kr  info@ncsc.go.kr |
| 대검찰청 | 인터넷범죄수사센터 | 02-530-4949 | www.spo.go.kr  icic@icic.sppo.go.kr |
| 한국인터넷진흥원 | 인터넷침해사고대응지원센터 | 118 | www.krcert.or.kr  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 |

## **2-4. 주요 전산장비, 통신회선 등의 이중화 구성도**



- 회선 이중화: KT Backbone Master, Slave로 회선 이중화, Master 회선에 문제 발생시 Slave 회선으로 무중단 서비스 가능

- 방화벽 이중화: Full Mash로 구성, 1번 방화벽(FW01)의 장애 시 2번 방화벽(FW02)을 통해 서비스를 하는 이중화 구조로 구성

- DB 이중화: 1호기 DB에서 장애 발생 시 이를 감지하여 VIP를 2호기 DB로 이동시키는 Failover 구성

# **3. 각종 프로그램 보유 현황**

## **3-1. 프로그램 보유 현황**

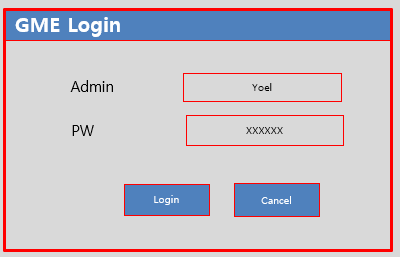
### **3-1-1. 프로그램 정의 및 목적**

* 정의: 모바일 기술과 금융결제 지식 등을 바탕으로 사용자들의 목적에 맞는 결제서비스
* 목적: 기업들의 다양한 비용 수납 서비스 환경 및 트렌드를 분석해 사용자의 목적에 맞는 서비스를 제공하는 것을 목적으로 합니다.

1. 전자지급결제 대행서비스: 이용자가 결제대금을 회사의 전자결제 시스템을 통하여 금융기관에 등록 정산을 대행하거나 매개하는 서비스

### **3-1-2. 프로그램 설명서**

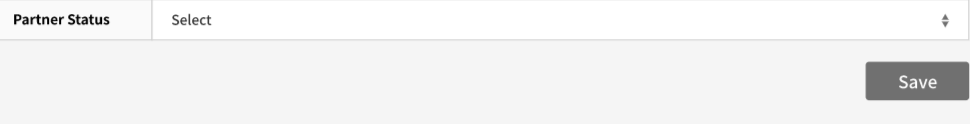
1. 로그인 화면



1. 파트너 신규 등록

테이블이(가) 표시된 사진

자동 생성된 설명



1. 파트너 조회 화면

테이블이(가) 표시된 사진

자동 생성된 설명

1. 자금관리 – 잔액관리화면

테이블이(가) 표시된 사진

자동 생성된 설명

1. 자금관리 – 입금추가화면



1. 자금관리 – 입금관리화면

테이블이(가) 표시된 사진

자동 생성된 설명

1. 자금관리 – 자금관리화면

테이블이(가) 표시된 사진

자동 생성된 설명

1. 거래 관리

텍스트이(가) 표시된 사진

자동 생성된 설명

### **3-1-3. 보유 프로그램 및 DB 목록**

1. 프로그램 목록

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 번호 | 업무명 | 프로그램 명 | ID | 용도 | 관련 DB Table | 개발언어 | 담당자 |
| 1 | GME PG | PGAuth | S-001 | 인증 | PG\_COMPANY | C# | 노설 |
| 2 | GME PG | PG-API | S-002 | 거래 | INBOUND\_REMIT\_TRAN | C# | Manoj Subedi |
| 3 | GME PG | PG-EXRATE | S-003 | 환율 | INBOUND\_COSTRATE | C# | Saroj Chalise |
| 4 | GME PG | PG-FUND | S-004 | 자금 | INBOUND\_APIUSER | C# | Maoj Subedi |
| 5 | GME PG | GME-CALC | S-005 | 정산 | INBOUND\_PARTNER\_SETTING | C# | 최재영 |
| 6 | GME PG | PG-KJ API | S-006 | 광주은행  API | VirtualAccountMapping | C# | 최재영 |
| 7 | GME PG | PG-KFTC API | S-007 | 오픈뱅킹 API | KFTC\_Customer\_master | C# | 최재영 |

1. DB 테이블 목록 및 정의서

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 번호 | 테이블 명 | 테이블 ID | 테이블 개요 | 개인정보 유무 | 암호화 여부 |
| 1 | PG\_PARTNER | DB-001 | 파트너 정보 | O | O |
| 2 | PG\_PARTNER\_USER | DB-002 | 파트너 유저 | O | O |
| 3 | PG\_EXCH\_HISTORY | DB-003 | 파트너 환전정보 | X | 해당사항  없음 |
| 4 | PG\_MEMBER | DB-004 | 파트너 상점정보 | O | O |
| 5 | PG\_DEPOSIT\_HISTORY | DB-005 | 파트너 입금정보 | X | 해당사항  없음 |
| 6 | PG\_SET\_HISTORY | DB-006 | 파트너 정산정보 | X | 해당사항  없음 |
| 7 | INBOUND\_TRAN\_RECEIVERS | DB-007 | 파트너 수신 테이블 | O | O |
| 8 | INBOUND\_TRAN\_SENDERS | DB-008 | 파트너 송신 테이블 | O | O |
| 9 | INBOUND\_TRAN\_INFO | DB-009 | 파트너 거래정보 테이블 | O | O |

1. IT팀 조직도

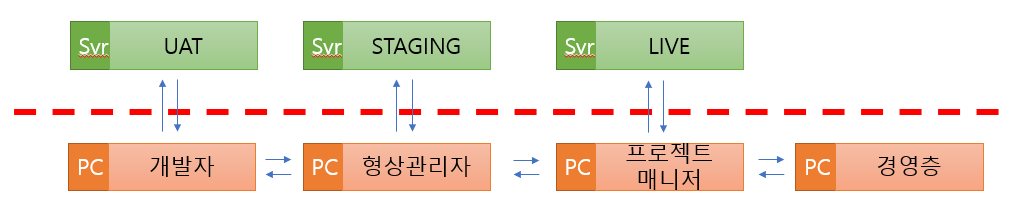


1. 업무분장표

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 번호 | 업무 | 업무 개요 | 이름 | 직위 |
| 1 | 형상 관리  서비스 운용  인프라 운영 | 개발 및 인프라 관련 전반적 의사결정  -프로그램 변경, 폐기 승인 | 김한성 | 팀장 |
| 2 | 서버 개발자 | 관리자설정, 파트너관리 | 노설 | 팀원 |
| 3 | 서버 개발자 | 파트너 연동 API | Manoj Subedi | 팀원 |
| 4 | 서버 개발자 | 거래내역관리 | Saroj Chalise | 팀원 |
| 5 | 서버 개발자 | 자금관리, 정산관리 | 최재영 | 팀원 |
| 6 | 클라이언트 개발자 | 파트너 조회 | 전태현 | 팀원 |
| 7 | QA | 프로그램 테스팅 및 품질관리 | Pheaktra They | 팀원 |
| 8 | QA | 프로그램 테스팅 및 품질관리 | 전인혁 | 팀원 |
| 9 | 보안 운영 | FSDC&본사 보안 취약점 및 장비 관리 | 이영우 | 팀원 |
| 10 | 보안 운영 | FSDC&본사 보안 취약점 및 장비 관리 | 정다연,  Ravindra Acharya | 팀원 |

## **3-2. 프로그램 등록, 변경, 폐기 절차**

개발 및 운영 유지보수 과정에서 변화되어가는 소프트웨어의 모습을 가시화해 짜임새 있고 질서　있게 통제함으로써 그 변경내용을 체계적이고 일관성 있게 수용하도록 한다.



### **3-2-1. 변경요청**

형상변경 요구서([별지1] 프로그램 수정/개발신청서)를 발의자가 작성한다.

### **3-2-2. 변경 수행 및 통제**

- 개발자는 개발사항에 대한 내용을 형상관리자와 협의한다.

- 형상관리자는 형상통제표준에 의거하여 형상관리를 처리한다.

- 프로그램 개발/테스트 이후 운영 서버로의 이관은 개발자를 제외한 제3자(PM)의 승인 절차를 거친다.

- (주)글로벌머니익스프레스는 형상관리 툴로 SVN을 사용하며, 형상관리를 위한 항목은 다음과 같다.

* 요구사항 명세서
* 설계/인터페이스 명세서
* 테스트 설계서
* 소스 코드

1. 형상통제표준

형상관리자는 품질관리자에게서 시정요구에 대한 문서를 받아 본 문서가 타당하다고 생각되면 그에 맞는 버전관리, 변경관리를 진행한다.

* 버전관리：　형상항목이 과거부터 현재에 이르기까지 변경이 진행됨에 따라 각 변경에 대해서 버전을 부여함으로써 히스토리를 관리
* 변경관리：　변경 요청사항에 대해, 비용 및 기간 등을 고려하여 변경의 타당성을 평가한 뒤, 타당한 경우 제품 또는 산출물을 변경하고, 그렇게 않을 경우 변경을 하지 않는 일련의 과정

1. 형상관리 역할

|  |  |
| --- | --- |
| 경영층 | * 프로젝트의 형상관리 활동에 대한 방침 제공 * 프로젝트의 형상관리 활동을 위한 필요한 자원과 자금 제공 * 형상관리 활동을 정기적으로 검토 |
| 프로젝트 매니저 | * 프로젝트의 형상관리 조직을 구성함 * 해당 프로젝트의 형상통제위원회 위원장의 역할을 수행 * 모든 형상 항목과 내부와 외부로부터 발생하는 모든 변경요청에 대한 최종 승인 권한을 가짐 * 형상 항목 및 베이스라인을 검토함 * 베이스라인의 배포를 승인함 * 프로젝트 형상관리 활동의 주요 사안에 대해 경영층에 보고함 |
| 개발자 | * 베이스라인으로 등록된 형상 항목을 사용하여 엔지니어링 활동을 수행 * 변경 요청 및 담당하는 형상 항목에 대한 변경을 구현 * 형상감사 결과 발생한 부적합에 대한 시정 조치를 수행 * 시큐어 코딩을 적용하여 개발 수행 |

1. 형상항목 선정

* 형상항목：　개발 프로세스에서 생산되거나 사용되는 작업 산출물 또는 작업 산출물들의 집합체　（Ｅｘ． 요구사항 명세서，　설계/인터페이스 명세서，　테스트 설계서，　소프트웨어 품질보증, 형상관리, V&V 계획서，　코드 모듈）
* 형상항목 선정： 관리 방법이나 변경에 대한 통제 여부에 따라 산출물을 구분하고, 이 중 변경에 대한 통제가 필요한 산출물을 선정하는 활동

4) 형상 상태 보고

* 베이스라인의 현재 상태 및 변경 항목들이 제대로 반영되는지 여부를 보고하는 절차
* 베이스라인으로 설정된 형상 항목의 구조와 변경 상태를 기록하여 보고함으로써, 형상 항목의 개발 상태에 대한 시각화를 제공
* 형상 상태 보고서: 형상 관리자가 작성하여 형상 관리 계획서에서 정한 주기대로 작성 및 제출, 상위 관리자에게 보고. 베이스라인의 상태, 변경 제어 상태, 형상 통제 위원회 활동 내역, 변경 요청의 상태 등을 담음.

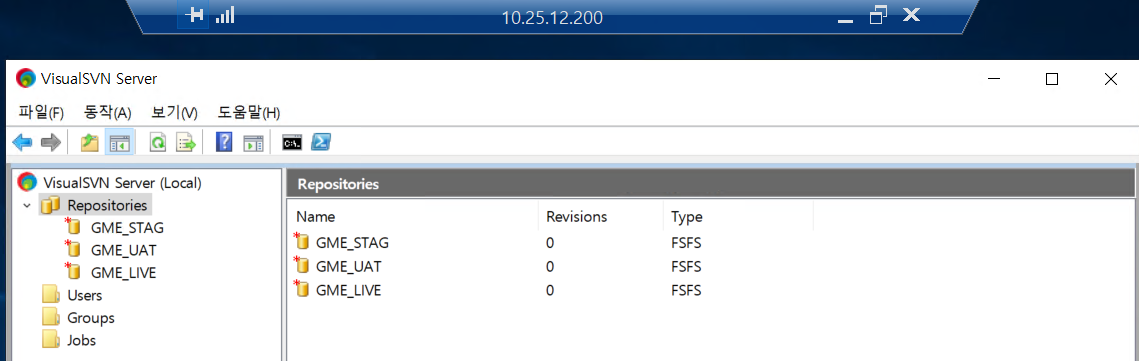
5) 형상 감사

- 형상 관리 계획서대로 형상 관리가 진행되고 있는지, 요구사항 문서대로 제품이 제작되었는지 감사하는 활동으로, 하기의 내용을 포함하여야 함.

* 모든 승인된 변경의 반영 여부
* 관련된 항목의 갱신 여부
* 승인되지 않은 변경의 반영 여부
* 인도될 항목과 요구사항, 디자인과의 일치 여부
* 모든 알려진 소프트웨어의 문제가 변경 승인에 의해 검토되었는지 여부
* 버전 기술 문서의 준비 여부

6) 형상 관리 툴

- 형상관리 서버는 내부망(10.25.12.200)에 위치하고 있으며, UAT, STAG, LIVE의 Repository를 별도로 운영하고 있다.

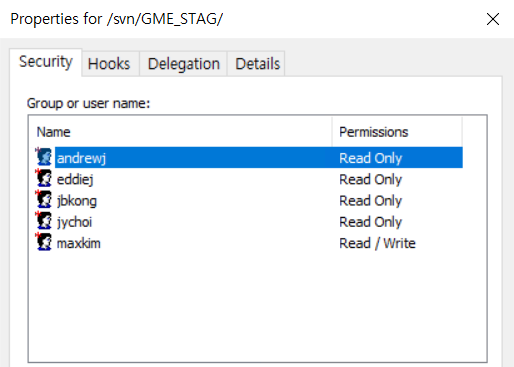


* 형상관리 서버는 지정된 중요단말에서만 접속이 가능하며, 등록된 계정의 사용자에 한하여 인증을 통한 접속이 가능하다.

테이블이(가) 표시된 사진

자동 생성된 설명

* STAGING Repository에는 형상관리자만 Read/Write가 가능하고, 개발자는 Read 만이 가능하다.



* LIVE Repository에는 PM만 Read/Write가 가능하다.

텍스트이(가) 표시된 사진

자동 생성된 설명

### **3-2-3. 응용 프로그램 폐기**

1. 운용자는 시스템 전환, 제도개선 등으로 프로그램 폐기사유가 발생하였을 경우 개발자에게 폐기 대상 프로그램 목록을 요청한다.

2. 개발자는 폐기 사유가 발생한 프로그램을 확인하여 운용자에게 프로그램 폐기 목록을 통보한다.

3. 운용자는 형상관리자에게 프로그램 폐기를 요청한다.

4. 형상관리자는 폐기 요청을 받은 경우 다음 각 목과 같이 처리한다.

* 폐기 프로그램을 형상관리시스템 내의 별도장소로 옮긴 후 기존 형상관리 디렉토리에서 삭제한다.
* 폐기 프로그램은 별도장소에 3년간 보관하며, 보관기간 중 개발자의 열람이 가능하도록 폐기 프로그램의 모든 버전을 관리한다.

### **3-2-4. 프로그램 관리 양식**

응용 프로그램 관리를 위해, 다음의 양식을 통해 프로그램의 변경/개발 요청을 관리한다.

[별지1] 프로그램 수정/개발신청서 작성예

테이블이(가) 표시된 사진

자동 생성된 설명

# **10-4. 정보처리시스템 관리방안**

## **4-1. 계정 및 비밀번호 부여절차**

정보처리시스템의 계정 및 비밀번호 부여절차는 다음과 같이 정의한다.

가. 계정 등록

- 사용자계정은 개인별로 부여한다.

- 사용자계정 등록 (신규, 추가, 해지) 신청서(별첨 1)를 작성하여 시스템관리 담당자에게 신청한다.

- 사용자 삭제 또는 권한 변경 사유가 발생한 경우, 삭제 또는 변경 신청서를 작성하여 통보하여야 한다.

- 시스템 관리 담당자는 검토, 승인 후 사용자 관리대장(별첨 2)에 기록하고, 사용자를 등록한 후 결과를 신청한 사용 부서에 통보한다.

- 계정은 각 사용자별로 부여하고 사용자 계정의 공동사용이 불가피한 경우 개인별 사용내역이 관리될 수 있도록 공동사용계정 현황 및 내역을 기록 관리한다.

- 시스템 관리 담당자는 월간 단위로 사용자 등록 및 변경 현황을 유지한다.

나. 사용자 계정의 재확인

- 휴직 및 퇴사여부, 업무 필요성 여부

- 마지막 사용일자가 60일을 넘겼을 경우

- 비밀번호가 없거나 비밀번호가 계정이름과 동일한 계정을 허용해서는 안 된다.

- 특별한 경우를 제외하고는 하나의 로그인 아이디는 한 번만 로그인 할 수 있다.

다. 계정 정지

- 비밀번호 오류 5회 이상 연속 발생 시 계정을 정지시킨다.

- 보안관리자에게 정지계정의 현황을 보고한다.

라. 정지된 계정의 재사용

- 다시 사용하는 사용자는 본인 확인 후 새로운 비밀번호를 부여받고, 최초로 로그인을 할 때, 즉시 비밀번호를 변경하도록 해야 한다.

마. 계정의 폐쇄

- 계정이 폐쇄되는 사유가 발생시에는 사유가 발생하는 즉시 삭제하도록 하며, 계정의 폐쇄는 아래의 사유에 따른다.

(1) 사용자가 탈퇴하는 경우

(2) 6개월 이상 미 사용 계정

바. 비밀번호 사용

- 신규 사용자에게 시스템 사용에 대한 권한을 부여할 때에는 반드시 비밀번호를 받도록 해야 한다.

- 모든 사용자는 비밀번호 인증을 통해서만 시스템을 사용할 수 있게 하여야 한다.

사. 비밀번호 관리

비밀번호는 다음 각 호 사항을 반영하여 숫자와 문자, 특수문자 등으로 9자리 이상으로 정하고, 분기 1회 이상 주기적으로 변경 사용하여야 한다.

- 사용자계정(ID)과 동일하지 않은 것

- 개인 신상 및 부서명칭 등과 관계가 없는 것

- 일반 사전에 등록된 단어는 사용을 피할 것

- 동일단어 또는 숫자를 반복하여 사용하지 말 것

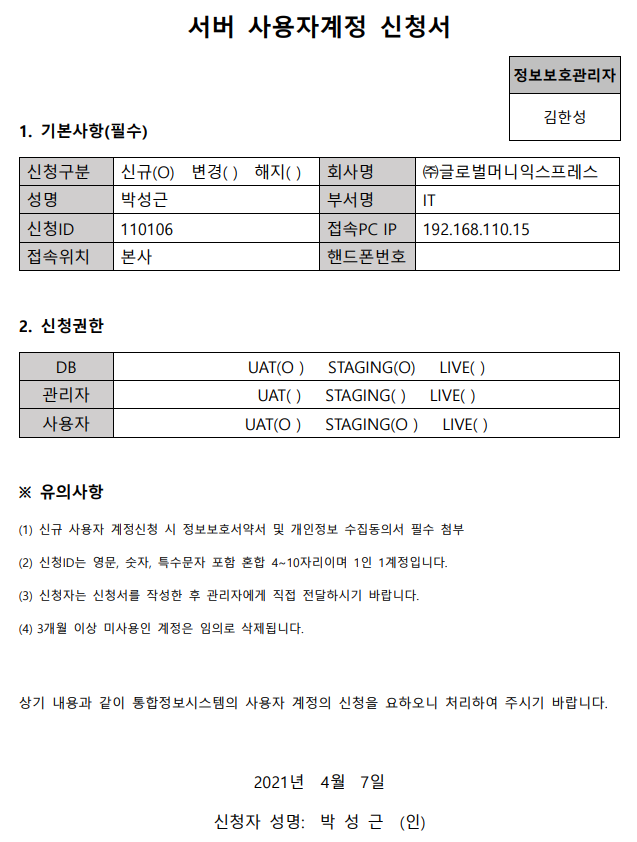
- 사용된 비밀번호는 재사용하지 말 것

- 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것

### **4-1-1. 계정 관리 양식**

정보처리시스템의 계정 관리를 위해, 다음의 양식을 통해 계정 생성/변경/해지와 그 현황을 관리한다.

[별지1] 계정신청서 작성예



[별지2] 서버계정관리대장 작성예

테이블이(가) 표시된 사진

자동 생성된 설명

## **4-2. 접근 권한 통제**

1) 관리 정책

- 응용프로그램 개발 담당자는 응용프로그램 사용자를 사용자별, 직책 별, 부서별 및 인가된 등급 등으로 접근 권한을 구분하여 설계한다.

- 응용프로그램개발담당자는 응용프로그램 사용자의 접근 권한 및 직무에 따라 필요한 화면 및 메뉴가 다르도록 설계한다.

- 응용프로그램개발담당자는 특별한 관리가 요구되는 중요 개인정보(주민등록번호, 비밀번호, 신용카드번호, 계좌번호 등) 또는 회사 정보(대외비, 비밀 문서 등)에 접근 시 유출 또는 삭제의 위험을 방지하기 위해 이용자 또는 사용자의 추가적인 인증 절차를 적용한다.

- 응용프로그램개발담당자는 필요한 경우 시간 및 IP 주소별로 이용자 또는 사용자의 접근을 통제할 수 있도록 설계한다.

- 오픈 API운영서버는 오직 서버 관리자만 접근 허용한다.

- 응용프로그램운영담당자는 응용프로그램운영관리자의 승인을 받은 후 사용자에게 접근 권한을 부여, 변경 및 회수한다.

- 응용프로그램운영담당자는 응용프로그램운영담당자 외 사용자가 응용프로그램 관리 화면, 파일 및 디렉터리 등 응용프로그램의 주요 정보에 직접 접근할 수 없도록 접근 통제한다.

- 응용프로그램운영관리자는 외부에서 관리자 전용 응용프로그램(관리자 웹 페이지, 관리 콘솔 등)에 접근 시 접근통제 대책을 수립해야 한다.

- 응용프로그램운영담당자는 응용프로그램의 정상적인 운영을 방해하거나 부정사용이 의심될 경우 해당 사용자의 권한을 제한한다.

- 정보보호담당자는 특수 권한 및 직무 별 권한 설정의 적절성 등에 대해 분기 1회 이상 점검한다.

- 사용자 계정 및 비밀번호 관리, 권한 관리 등 접근통제에 대한 세부사항은 ‘접근통제 관리 지침’에 따른다.

2) 접근 권한 관리 현황

① 서버 통제

- 팀장은 DB 사용자의 접근 권한을 사용자별, 직책 별, 부서별 및 인가된 등급 등으로 구분하여 부여한다.

- 팀장은 부정사용이 의심될 경우 해당 사용자의 권한을 제한한다.

- 접근 시 항상 IPsec VPN 및 OTP 인증의 2depth 인증을 거치도록 한다.

- Root 권한 및 특수 권한 계정은 별도로 기록하여 내화금고에 보관하도록 한다.

- Guest 계정은 비활성화한다.

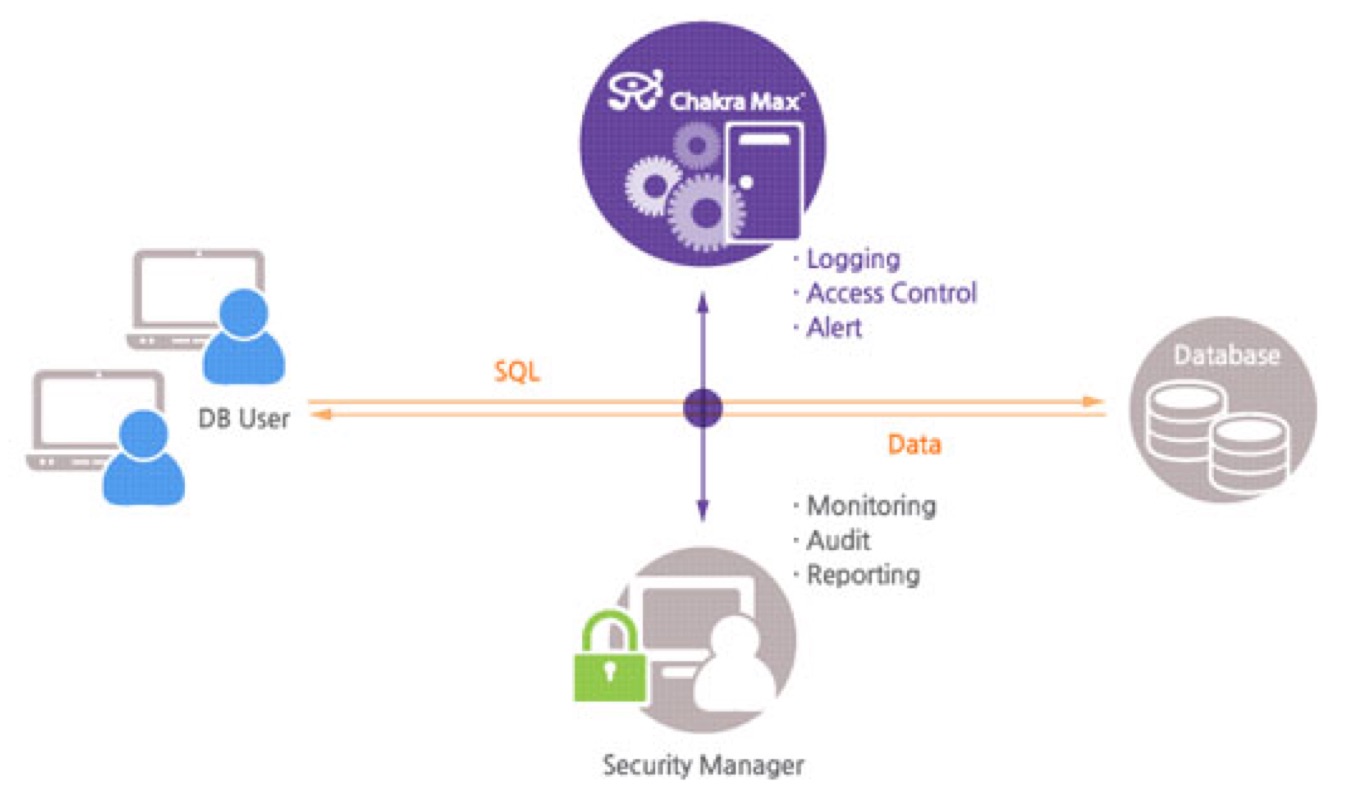
- 보안 감사 로그는 정보보호담당자가 월 1회 이상 점검한다.

② DB 통제

- 팀장은 DB 사용자의 접근 권한을 사용자별, 직책 별, 부서별 및 인가된 등급 등으로 구분하여 부여한다.

- 팀장은 부정사용이 의심될 경우 해당 사용자의 권한을 제한한다.

- DB 접근 현황, 접속 세션, 트래픽, SQL에 관한 감사 로그를 생성하기 위해 접근제어 솔루션인 Chakra Max를 활용한다.



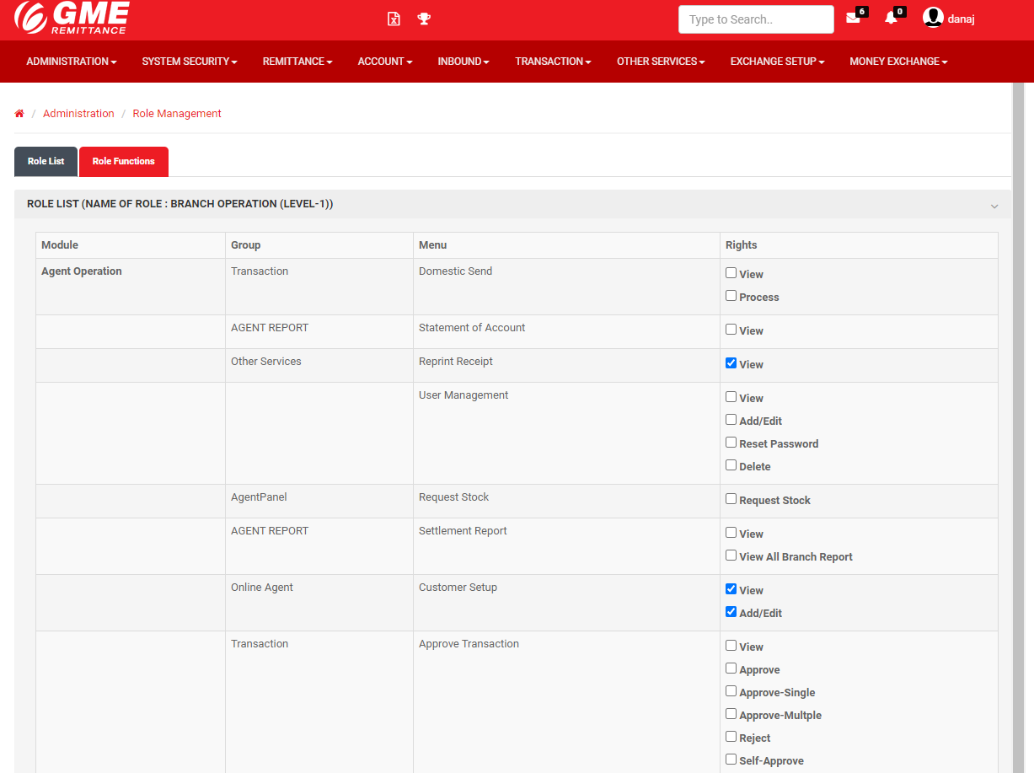
Chakra Max에서 생성된 감사 로그는 정보보호담당자가 월 1회 이상 점검하며, 2년 간 보관 및 관리한다.

① 관리자 페이지

사용자의 Role에 따라 권한을 다르게 부여하여, 불필요한 권한이 주어지지 않도록 한다.

테이블이(가) 표시된 사진

자동 생성된 설명



## **4-3. 전산자료 반출입 통제**

전산자료의 반출입 절차는 다음과 같이 정의한다.

텍스트, 시계이(가) 표시된 사진

자동 생성된 설명

* + 전산 자료 반출입을 원하는 사용자는 다음의 사항을 준수한다.
  + 전산 자료 반출입 신청서(4-3-1. 전산자료관리양식 [별첨 1])를 작성하여 시스템관리 담당자에게 신청한다.
  + 시스템 관리 담당자는 검토, 승인 후 전산 자료 관리대장(4-3-1. 전산자료관리양식 [별첨 2])에 기록하고, 승인 혹은 반려하여 사용자에 통보한다.

### **4-**3-1. 전산자료 관리 양식

전산자료의 반출입 통제를 위해, 전산 자료는 다음의 양식을 통해 반출입과 그 현황을 관리한다.

[별지1] 전산자료반출입신청서 작성예

테이블이(가) 표시된 사진

자동 생성된 설명

[별지2] 전산자료관리대장 작성예

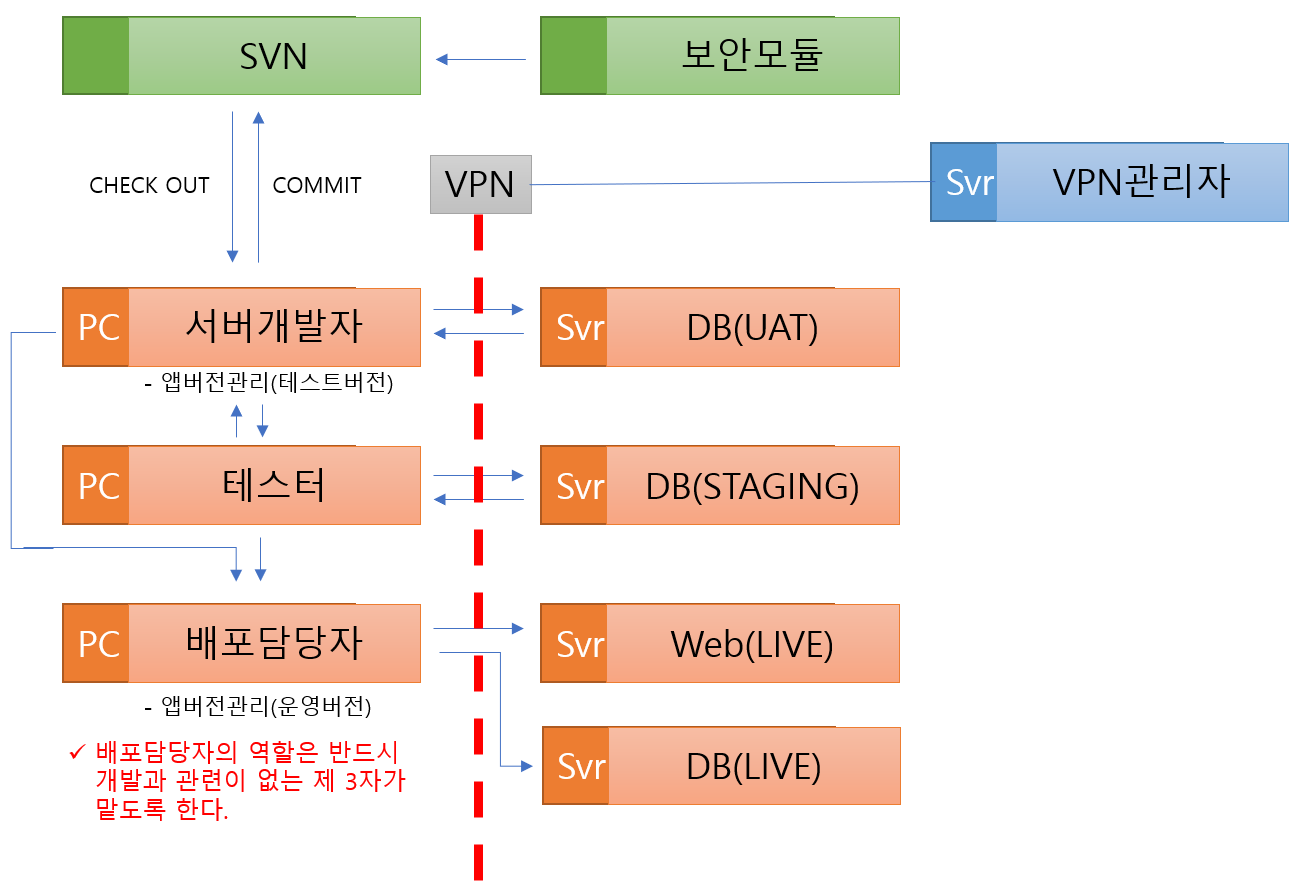
테이블이(가) 표시된 사진

자동 생성된 설명

## **4-4. 전산 개발 규정**

### **4-4-1. 개발/테스트/운영 환경 및 업무 분리**

응용 프로그램 개발 팀의 업무 흐름은 다음과 같이 정의한다. 개발자와 테스터, 배포담당자는 직무를 분리하여 각기 다른 인물이 역할을 수행하도록 한다.



|  |  |
| --- | --- |
| 환경 | 내용 |
| Local 개발 환경 | 개발자 PC에 개발 및 테스트 환경이 셋업 되어 있는 환경　(예. 각 PC에 Visual Studio, Eclipse 와 같은 개발　툴과 컴파일러 등이 설치되어 있는 환경) |
| UAT 개발 환경 | 각 개별 개발자들이, 만든 코드를 합쳐서 서버 환경에서 테스트해볼 수 있는 환경. (IIS 및 MS-SQL 이 설치되어 있는 환경) |
| STAGING 환경 | 운영 환경과 거의 동일한 환경을 만들어 놓고, 운영환경으로 이전하기 전에, 여러 가지 비 기능적인 부분 (Security, 성능, 장애　등)을 검증하는 환경이다. |
| Production（Ｌｉｖｅ）운영 환경 | 실제 서비스를 위한 운영 환경 |

### **4-4-2. 보안 요구사항 분석 및 개발**

응용 프로그램 개발에 있어 다음과 같은 정책을 적용한다.

- 응용프로그램의 신규 개발 또는 변경을 위한 요구 분석 단계에서 보안요건을 분석하여 개발하고자 하는 응용프로그램에 구현되도록 한다.

- 요구분석 단계에서 응용프로그램 별로 필요한 보안 기능을 보안 담당자와 협의하여 정의하여야 하며, 보안 기능은 기존 시스템과 연동성 및 기 적용된 보안기능을 고려하여 정의하여야 한다.

- 응용 프로그램 개발 시 취약점이 발생하지 않도록 시큐어 코딩이 적용되어야 한다.

- 개발된 프로그램을 운영환경에 이관하기 전, 보안담당자에 의해 보안 취약점 점검이 실시되어야 한다.

- 개인정보처리시스템은 이용자의 개인정보 등 민감한 정보가 노출되지 않도록 비식별처리(마스킹 등)하여 출력되도록 한다.

- 개인정보 보관 시 암호화를 적용하며, 주요 정보 입력시에는 보안 키패드를 적용하도록 한다.

### **4-4-3. 응용프로그램 테스트 및 테스트 데이터 통제**

개발된 응용 프로그램의 테스트에 있어 다음과 같은 정책을 적용한다.

- 모든　테스트에　있어　실　데이터가　아닌　임의의　데이터를　사용하며，　대량의 테스트 데이터가 필요한 경우에는　난수　발생　함수를　사용하여　데이터를　생성한다．

- 개발자는 응용 프로그램을 운영 환경에 설치하기 전에 테스트 환경에서 테스트 과정을 거쳐야 한다.

- 개발자는 테스트 수행 시 사용된 테스트 데이터 및 관련 정보를 테스트 목적 달성 시 삭제하여야 한다.

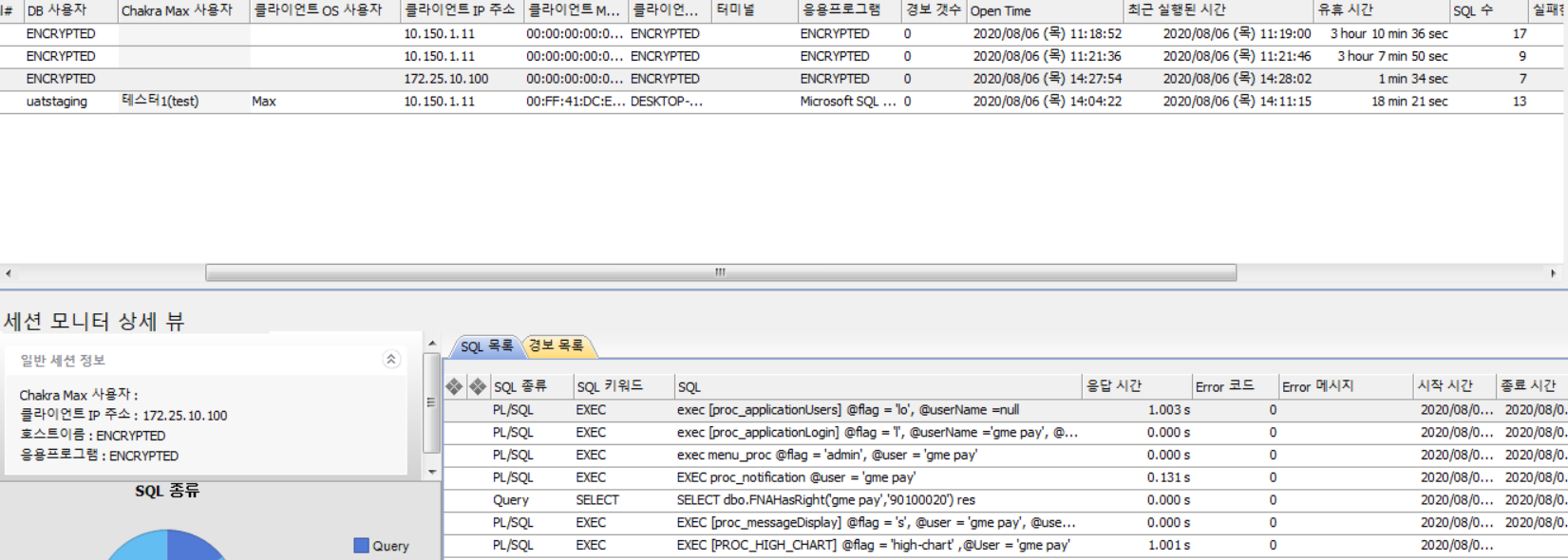
### **4-4-4. 응용 프로그램 이관**

응용프로그램　개발　및　변경의　목적과　적절성，　테스트　결과， 보안　취약성　검증내역을　종합하여　개발자가 아닌 제3자(팀장)의　승인　하에　이관을　실행한다．

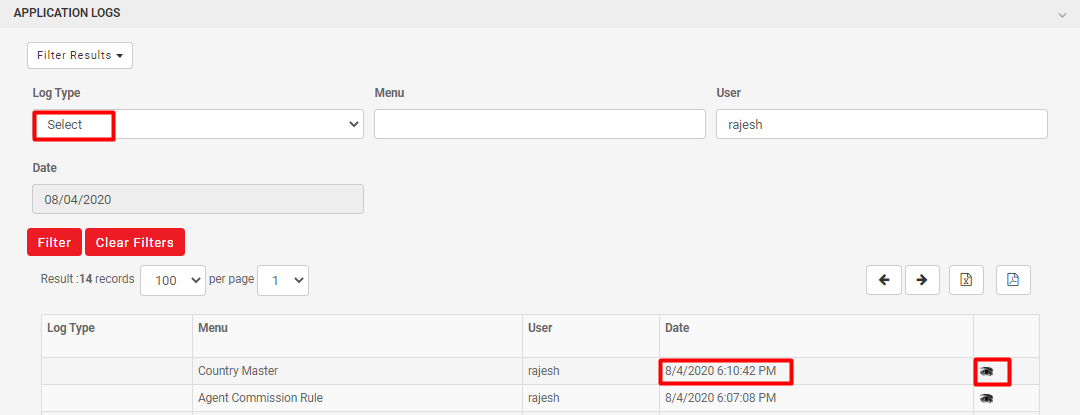
## **4-5. 접근기록 자동관리**

### **4-5-1. 중요정보 조회 시**

웹페이지를 이용해 데이터를 쿼리할 시, ChakraMax DB 접근제어 솔루션이 상세 로그를 저장한다. 누가, 언제, 어떤 쿼리를 실행했는지 확인할 수 있다.



웹 페이지를 이용해 중요정보를 쿼리하면, 관리자 페이지를 이용해 누가, 언제, 어떤 메뉴를 실행했는지 확인할 수 있다.



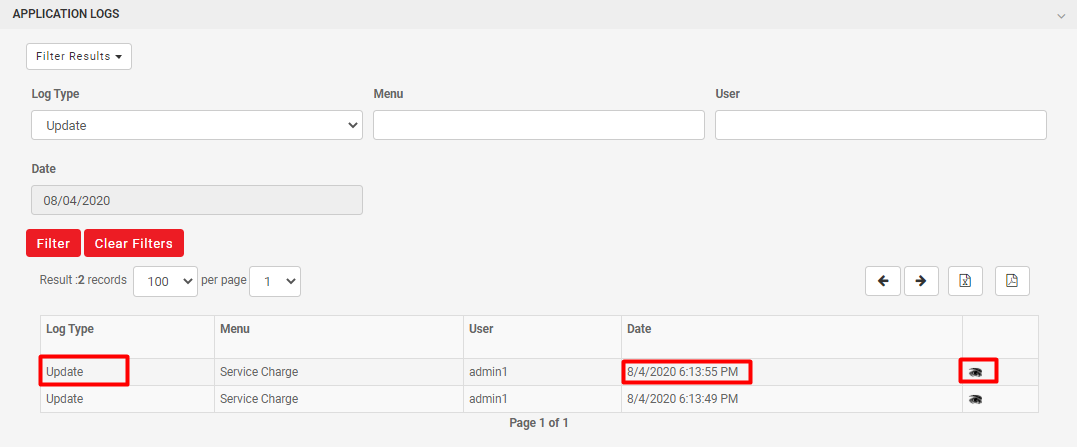
DB Management Tool(SSMS등)을 이용해 데이터를 쿼리하면, ChakraMax DB 접근제어 솔루션이 상세 로그를 저장한다. 누가, 언제, 어떤 쿼리를 실행했는지 확인할 수 있다.

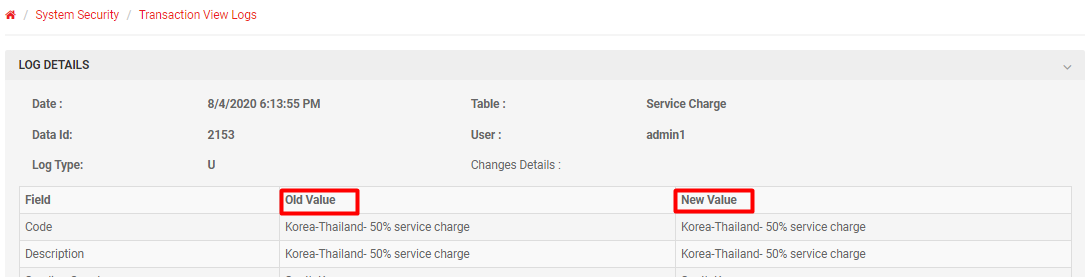
테이블이(가) 표시된 사진

자동 생성된 설명

### **4-5-2. 중요정보 수정 시**

웹 페이지를 이용해 데이터를 변경하면, 상세 로그를 저장한다. 관리자 페이지를 이용해 누가, 언제, 어떻게 데이터를 변경했는지 확인할 수 있다.





DB Management Tool(SSMS)을 이용해 중요정보의 데이터를 변경할 시, ChakraMax DB 접근제어 솔루션이 상세 로그를 저장한다. 누가, 언제, 어떤 쿼리를 실행했는지 확인할 수 있다.



## **4-6. 공개용 웹서버 보호**

DMZ에 위치한 공개용 웹서버로 접근하는 트래픽은 방화벽과 IPS 장비를 통해 제어 및 필터링하며, 운영에 있어 보안관제 전문업체인 ㈜Wins의 관제 서비스를 이용한다. IPS의 패턴을 통해 웹서버 해킹 시도가 차단되며, 모니터링을 통해 DDoS를 비롯한 각종 공격에 대한 실시간 대응이 가능하다. 또한 중대한 신규 취약점이 발표될 시 메일링 서비스를 통해 알려주며, 발생한 공격의 통계 정보를 월 단위로 리포팅한다.

텍스트이(가) 표시된 사진

자동 생성된 설명

## **4-7. 공개용 웹서버 계정 부여 현황**

|  |  |  |
| --- | --- | --- |
| 웹서버 종류 | 계정이름 | 직원명 |
| PROD-API-01 | GMEREMIT\MaxKim | 김한성 |
| GMEREMIT\Danaj | 정다연 |
| PROD-SMS-01 | GMEREMIT\MaxKim | 김한성 |
| GMEREMIT\Danaj | 정다연 |
| GMEREMIT\Danaj | 정다연 |
| GMEREMIT\Eddiej | 전인혁 |

## **4-8. 개인정보 유출 방지**

### **4-8-1. 개인정보 보유현황**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 개인정보파일 명칭 | 개인정보의 종류 | 개인정보의 주체수 | 부서명 | 개인정보취급자 |
| 고객마스터DB | 이름  비밀번호  고유식별번호  계좌번호  휴대폰번호 | 약 16만 건 | IT 팀 | 김한성 팀장 |

### **4-8-2. 개인정보 유출 방지**

텍스트이(가) 표시된 사진

자동 생성된 설명

- 고객마스터DB 내 개인정보는 AES256 알고리즘으로 암호화한다.

- 데이터베이스 접근 통제: Chakra Max DB접근제어 솔루션을 이용해 데이터베이스의 접근 현황과 사용자 식별정보를 감사하여, 유사시 개인정보 유출 경로의 추적이 가능하도록 한다.

- 개인정보에 접근한 모든 정보시스템 로그는 2년 이상 보관한다.

- 모든 중요단말 및 인터넷단말에 개인정보보호시스템인 지란지교 오피스키퍼 DLP 제품을 설치함으로써, 개인정보의 유출을 탐지하고, 미인가 이동식저장매체로의 복사 및 출력을 강력히 통제한다.

- 지란지교 오피스키퍼 DLP 제품 정책 설정을 통해 중요단말망 내 단말기들의 USB 이용을 차단하며, 중요단말망에서 인터넷망으로 자료를 반출하는 경우 망연계 솔루션의 기능을 통하여 자료를 반출한 해당 사용자명과 파일이 모두 로깅 되도록 한다.

## **4-9. 취약점 점검**

### **4-9-1. 점검 목적**

운영 중인 전자금융기반시설 및 서비스에 대하여 비인가자의 관점에서 취약점 진단 및 모의 해킹을 수행해 발견된 취약점이 서비스 및 시스템에 미치는 영향을 파악함으로써, 침해사고를 예방하고 서비스의 안정성을 확보한다.

### **4-9-2. 점검 대상 및 주기**

공개 모바일 앱 서비스인 GME Remit (Android/iOS), 공개 웹 서비스(URL: [www.gmeremit.com](http://www.gmeremit.com) )에 대하여 연 2회(6개월에 1회) 정보보호전문기업인 ㈜시큐어원으로부터 모의해킹 서비스를 받는다. 이외 서버, DBMS, WEB/WAS, 네트워크장비, 보안장비에 대해 연 1회 전자금융기반시설 취약점 점검 서비스를 받는다.

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

### **4-9-4. 점검 항목**

점검은 금융보안원에서 발표된 ‘전자금융기반시설 보안 취약점 평가기준(제2021-1호)’ 항목을 기준으로 실시한다.

# **10-5. 감시운영체제 구축 현황**

## **5-1. 정보보호시스템 구축 현황**

### **5-1-1. KT IDC 정보보호시스템 구축 현황**

대고객 서비스의 정보보호를 위해 IDC에 다음과 같은 보안 장비들을 구축하고 운영한다.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 구분 | 벤더 | 모델명 | 제원 | 수량 | 기능 |
| F/W | Wins | Sniper  AP2000 | CPU 2Core 3.5GHz  Memory 4GB  HDD 1TB  CF Memory 4GB  NIC 1GF \* 4port, 1GC \* 8port  Power Dual  Throughput 6Gbps | 2 | 방화벽 |
| IPS | Wins | Sniper  One-I 1000 | CPU 4Core 3.5GHz  Memory 32GB  HDD 2TB  CF Memory 4GB  NIC 1GF \* 2port, 1GC \* 4port  Power Dual  Throughput 4Gbps | 2 | 침입방지시스템 |
| IPsec VPN | FutureSystems | XTM1000F | CPU 2Core 700MHz Memory 1GB HDD N/A CF Memory 4GB NIC 1G \* 8port Concurrent Session 500,000 CPS 15,000 Power Single | 1 | KT IDC-HQ(본사) 중요단말망 연결용 IPsec VPN (방화벽 기능 포함) |

특히, 방화벽 및 IPS 장비의 운영에 있어서는 보안관제전문업체인 ㈜Wins의 관제 서비스를 이용한다. IPS의 패턴을 통해 웹서버 해킹 시도가 차단되며, 모니터링을 통해 DDoS를 비롯한 각종 공격에 대한 실시간 대응이 가능하다. 또한 중대한 신규 취약점이 발표될 시 메일링 서비스를 통해 알려주며, 발생한 공격의 통계 정보를 월 단위로 리포팅한다.

텍스트이(가) 표시된 사진

자동 생성된 설명

### **5-1-2. 본사 정보보호시스템 구축 현황**

업무환경 정보보호를 위해 본사에 다음과 같은 보안 장비들을 구축하고 운영한다.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 구분 | 벤더 | 모델명 | 제원 | 수량 | 기능 |
| IPsec VPN | FutureSystems | XTM1000F | CPU 2Core 700MHz Memory 1GB HDD N/A CF Memory 4GB NIC 1G \* 8port Concurrent Session 500,000 CPS 15,000 Power Single | 1 | KT IDC-HQ(본사) 중요단말망 연결용 IPsec VPN (방화벽 기능 포함) |
| F/W | Fortinet | Fortigate 100D | CPU 4Core  Memory 3.8GB  HDD 32GB  Latency 37 ms | 1 | 인터넷망 방화벽 |
| NAC | Genian | Smart NAC | CPU Cerelon  Memory ４GB  HDD 64GB | 2 | 중요단말망/인터넷망 네트워크 접근통제 센서 |
| DLP | 지란지교 | Office Keeper | CPU : Intel® E2224 (3.4GHz)  Memory : 8Gb DDR4  HDD : SATA 1TB\*2 | 2 | 중요단말망/인터넷망 정보유출방지 서버 |
| 백신 | Ahnlab | HP HPE DL20 Gen10 | CPU 4core 3.3GHz  Memory 16GB\*2  HDD 2.1TB\*2  NIC 1G \* 2ports  Power Single | 1 | 인터넷망 백신 업데이트 서버 |
| 망연계 | SoftwithSolution | Crossnet | Intel® Pentium® Gold G5400 Processor (2Core, 3.70GHz)  DDR4 8GB UDIMM  128GB M.2 SSD  1TB S-ATA3 7.2krpm Disk (RAID)  Intel i211-AT, 6 x 1GbE RJ45 LAN ports  250W Single PSU | 2 | 중요단말망/인터넷망 망연계 서버 |

## **5-2. 망분리 현황**

DMZ에는 고객의 서비스 이용을 위한 웹 서버만을 두며, DB 서버, WAS 서버, 개발 서버는 내부망에 위치시킨다. 내부망은 중요단말기를 통해서만 접속할 수 있다.

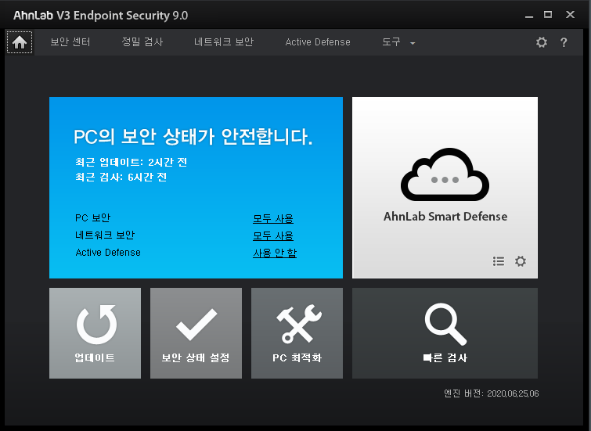
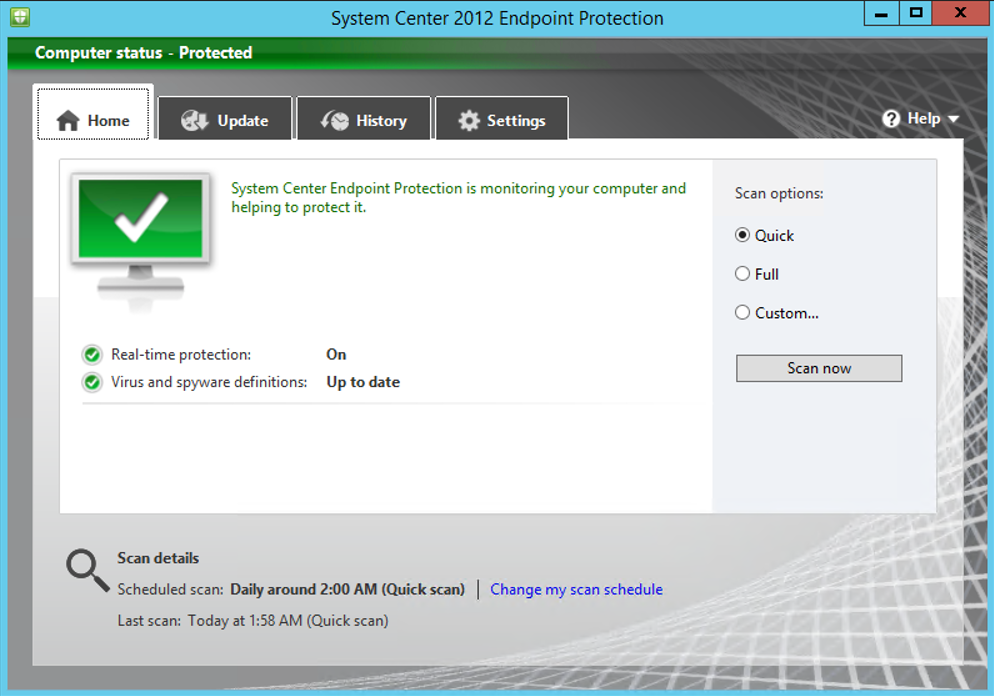
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 위치 | 구분 | Server | Internal IP | description |
| 내부 | DB | PROD-DB-001 | 10.25.10.151 | 운영 DB Server (1호기) |
| PROD-DB-002 | 10.25.10.152 | 운영 DB Server (2호기) |
| 내부 | DEV | UAT-DB-01 | 10.25.12.100 | 개발 DB Server |
| STAG-DB-01 | 10.25.10.60 | 테스트 DB Server |
| SVN-SVR-01 | 10.25.12.200 | 형상관리 서버 |
| 내부 | 업무시스템 | PROD-CORE-02 | 10.25.12.250 | 운영 관리자 페이지 |

텍스트, 장치, 저울이(가) 표시된 사진

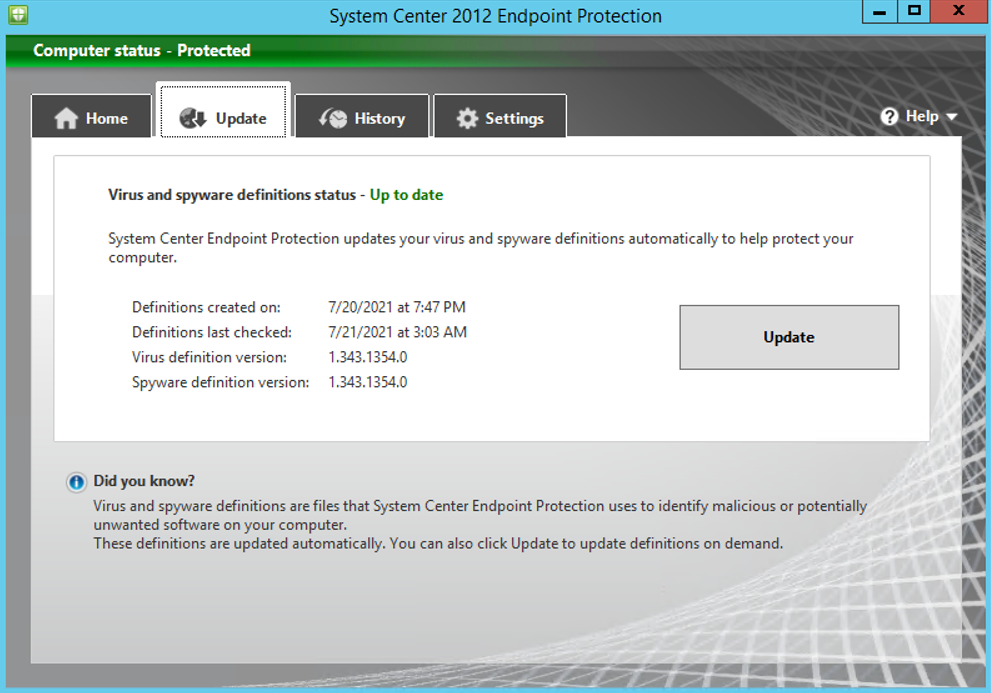
자동 생성된 설명

## **5-3. 악성코드 감염 방지대책**

모든 운영서버에 Microsoft System Center 2012 Endpoint Protection 백신 제품을 설치하였으며, 사용자 PC(업무망, 인터넷망)에 Ahnlab V3 Endpoint 백신 제품을 설치하였다.

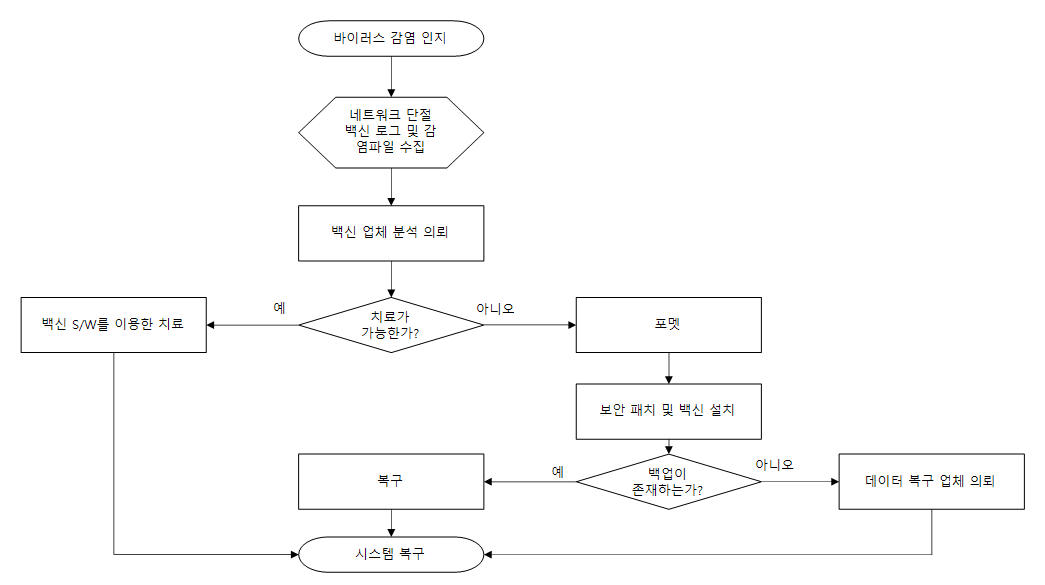


백신 제품의 패턴 업데이트 정책은 다음과 같다. Microsoft System Center는 매일 새벽 3시경 최신 패턴을 체크하고 업데이트하며, V3는 인터넷망 단말 기준 매 1시간 주기로 자동 업데이트를 받는다. 중요단말기는 각 단말의 담당자가 제조사에서 제공하는 패치 파일을 망연계 제품으로 반입하여 패턴을 업데이트 한다.



|  |  |
| --- | --- |
| V3정책 | 설정 값 |
| PC 실시간 검사 | 사용 |
| 악성코드 감염 파일 | 치료 |
| CD/USB 드라이브 자동 실행 방지 | 사용 |
| USB 드라이브 자동 검사 | 사용 |
| V3 무결성 정기 검사 | 사용 |
| V3 제품 보호 | 사용 |
| 사용자 진단 로그 보관 기간 | 90일 |
| 사용자 이벤트 로그 보관 기간 | 90일 |
| 검역소 보관 기간 | 90일 |
| 자동 업데이트 주기 | 1시간 |

악성코드 감염사례 발생 시 대응을 위한 복구절차는 다음과 같다.



# **10-6. 전산실 안정성 확보 및 보안대책**

## **6-1. 전산실 설비 목록**

다음 시설이 구비된 KT IDC에서 주요 전산시스템을 운용하고 있다.

텍스트이(가) 표시된 사진

자동 생성된 설명

## **6-2. 비상대책**

KT IDC 센터는 홍수, 지진 등 자연 재해를 대비하여 주요 전력 설비를 3층에 배치하였고, 2층과 3층간에 지진에 대비한 면진층을 구축하였다. 따라서 지진이 발생할 경우에도 면진층이 충격을 흡수하여 3층 이상에 있는 전력 설비 및 서버를 안전하게 보존한다.

## **6-3. 보호구역 지정 현황**

주요 전산시스템을 KT 목동IDC에 구축함으로써 CCTV, 출입통제를 통한 보안 안정성을 확보하였다. KT 목동IDC는 ISMS 정보보호 관리체계 인증으로 안정성을 인증 받은 시설이다.

텍스트, 스크린샷, 전자기기, 컴퓨터이(가) 표시된 사진

자동 생성된 설명

또한 본사 내 전산실 입구에 ‘통제구역’ 팻말을 부착하고, CCTV, 서버실 도어락을 설치하여 보안 안정성을 확보하였다.

## **6-4. 전산실 출입자 관리 기록**

KT IDC는 다음의 양식으로 방문자를 관리한다.

테이블이(가) 표시된 사진

자동 생성된 설명

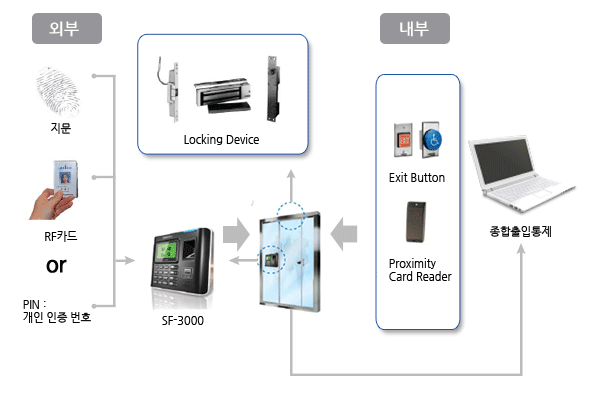
본사는 다음 양식의 수기명부를 작성하도록 하여 전산실 출입자를 관리한다.

테이블이(가) 표시된 사진

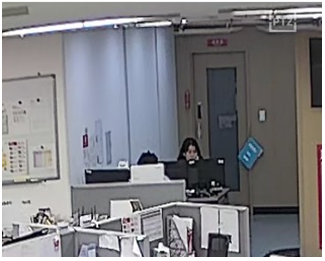
자동 생성된 설명

## **6-5. 출입자 감시장치 운영현황**

KT IDC에 적용되어 있는 물리보안 장치는 다음과 같다.



본사에 적용되어 있는 물리보안 장치로는 CCTV, 전산실 출입구 도어락이 있다.

 텍스트이(가) 표시된 사진

자동 생성된 설명

## **6-6. 전산실 배치도**

KT IDC의 물리 인프라는 다음과 같다.



글로벌머니익스프레스는 다음과 같이 KT와 코로케이션 서비스를 계약하였다.

텍스트이(가) 표시된 사진

자동 생성된 설명