Information Protection Manual for R&D Executives and Staff Members

HMG R&D CENTER

HYUNDAI
MOTOR GROUP

Contents

Access (persons/vehicles/equipment)

05 Information on the use of the Namyang Access Security System

08 How to install the mobile Namyang access security system

09 How to reserve a visit through a mobile device

10 Photographing procedure

11 Temporary cover removal procedure for new cars

12 Research institute access procedure for vehicles (staff members/partner companies/vehicles for testing purposes, etc.)

14 Sticker issuance procedure for vehicles owned by executives and staff members

15 Procedure to bring out the vehicle for testing purposes

17 How to access using a private vehicle by injured patients and handicapped staff members

18 Access procedure for visitors (how to make a reservation for a visit)

23 Access procedure for visitors during weekends

24 Research institute access procedure for employees of partner companies

25 Visitor's laptop computer approval procedure

28 Access procedure for Uiwang research institute

29 Restricted areas/how to apply for access permission

30 Research institute access procedure for executives and staff members working in other areas

31 Access procedure for security areas in the research institute (Design building/PDI building/quality assurance building)

32 Access procedure for staff members employed locally by the overseas research institute

33 Procedure for bringing in/out general articles again

38 Procedure for bringing in/out computer equipment

42 Employee ID card reissuance procedure

43 Access pass issuance procedure for employees of our affiliated companies working in the research institute

44 Access pass issuance procedure for dispatched workers, GE, and other company employees working inside the research institute

Technology (PC/Network)

46 Integrated PC management system(AD)

48 DRM (Digital Rights Management (document security))

53 OTP (One Time Password)

55 Secure USB

57 VPN & VDESK

60 Access Security Permission Application System (SRMS)

Management (education/inspection)

65 Status of security-related business standards

66 Major security-related Acts

68 Daily security for the research institute

69 How to report on a security accident and handling procedure

71 How to classify and indicate document security levels

72 Security pledge for executives and staff members
(Pledge for Trade Secret Protection / Pledge for National Core Technology Protection)

74 How to carry out the self-diagnosis of team security level

77 How to prepare the information asset classification standard sheet

78 Roles of the team security manager

79 How to change the team security manager

80 Computer equipment and work data transfer procedure at the time of dispatch/transfer

82 Matters of security to be observed at the time of retirement

83 Resident employee's data transfer procedure

89 How to collect the security pledge from a partner company

90 Security procedure and matters to be observed for employing a service

92 Security procedure in case of distribution/publication to the outside such as a paper presentation and a lecture held outside the company

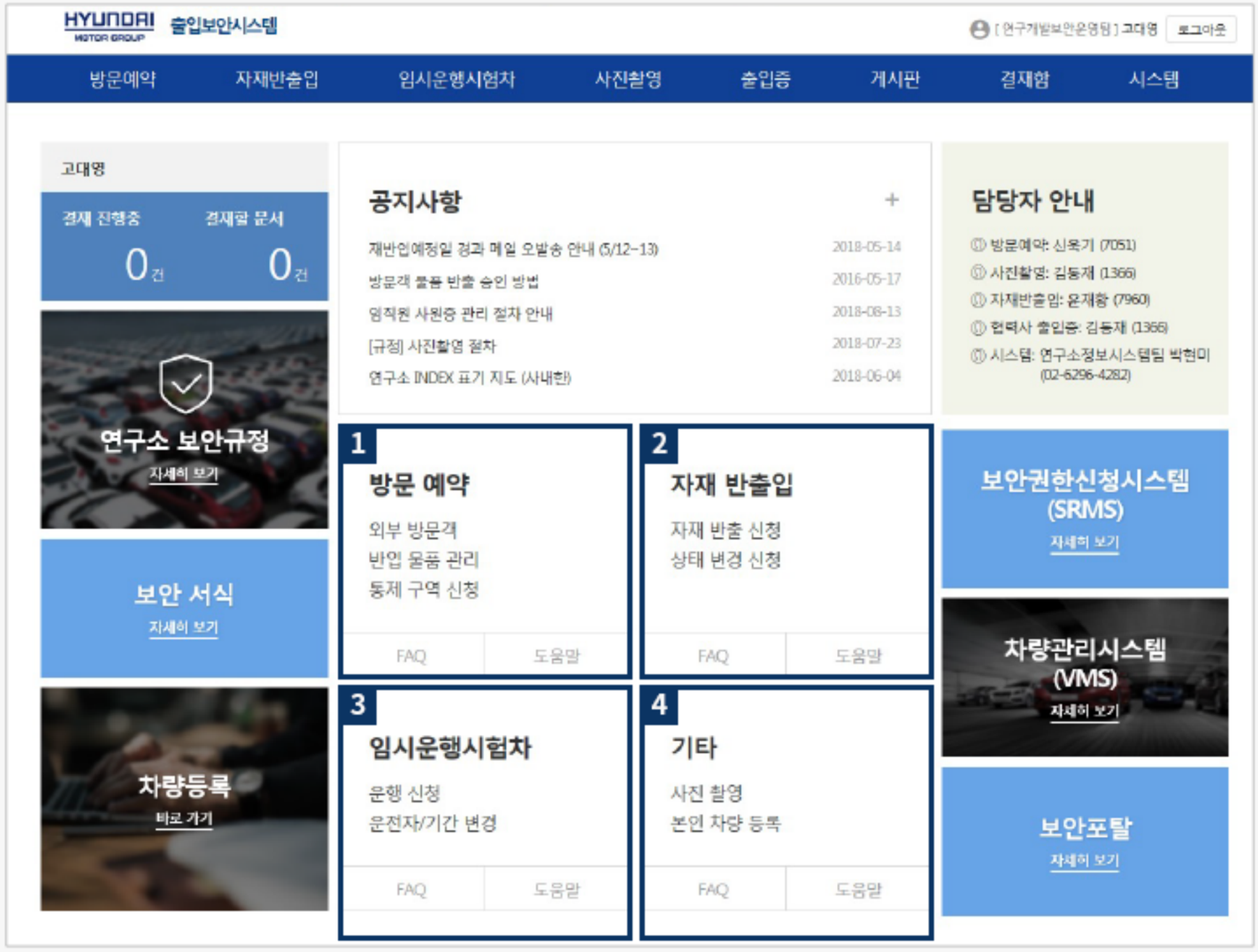
93 Security guide for external materials such as external paper presentations and lectures

94 How to use a shared folder and security matters to be observed

1 | Access (persons/vehicles/equipment)

Information on Using the Namyang Access Security System

You can apply for the reservation for a visit, bringing in and out of materials, management of test vehicles operated temporarily, photographing and access pass in the Namyang Access Security System.



1 Reservation for a visit : Visitor application and approval management

2 Bringing in and out of materials : Paid/free/re-bringing in and out application and approval management

3 Temporarily operated test vehicles : Application for operation, change of driver and period

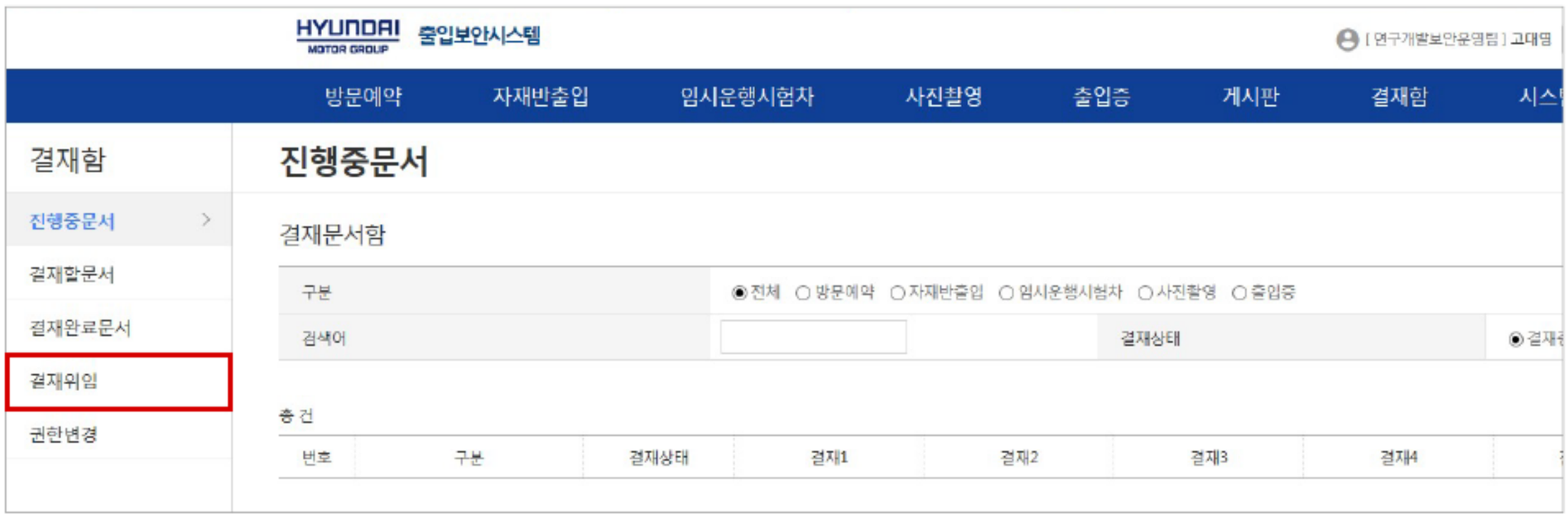
4 Others: application for photographing and the registration of own vehicle

FAQ

Q1. How can I request for the designation of an alternative approver for bringing in and out of materials?

1. Click Approval Box from Namyang Access Security System > Top Menu
(Only available for team managers or higher positions)

2. Click 'Approval Delegation' on the left menu



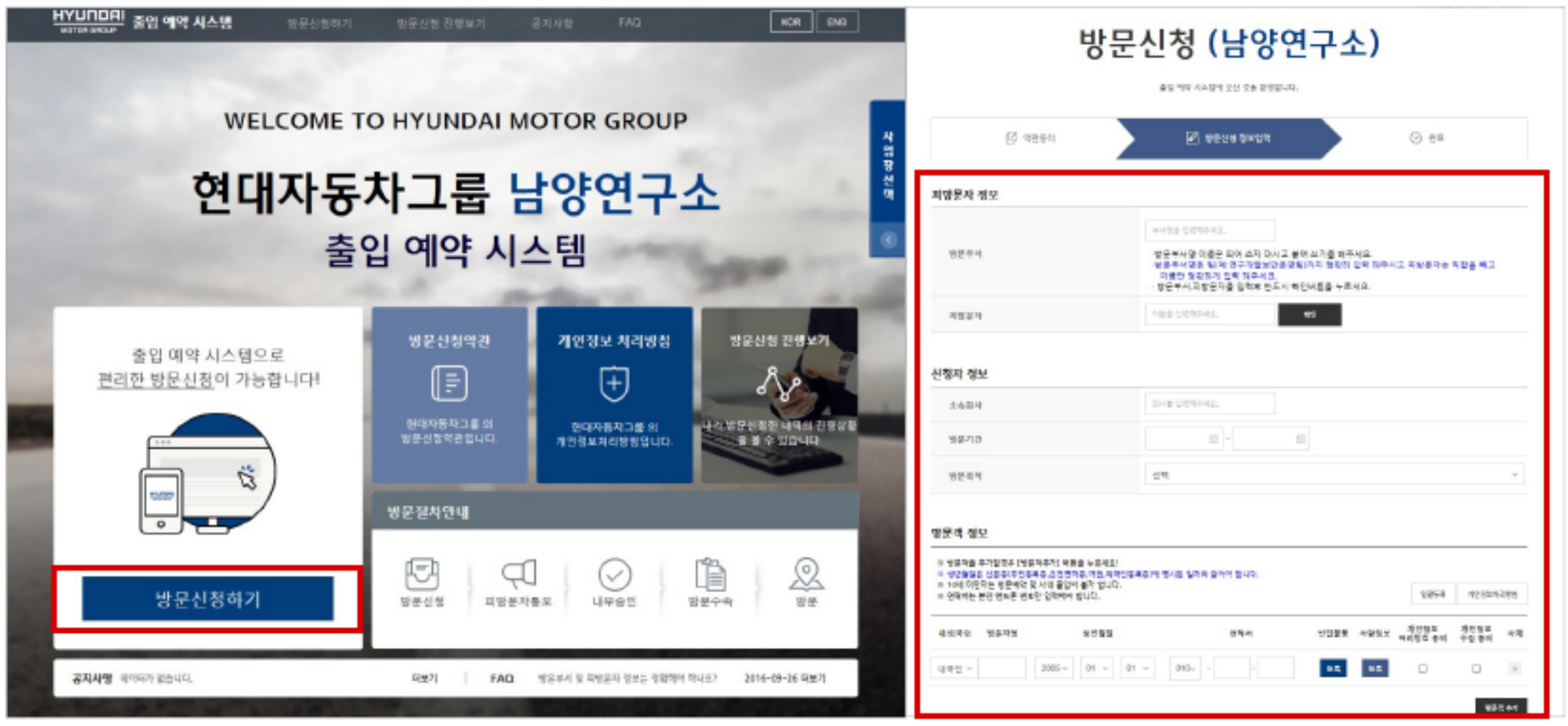
3. Click the existing [Inquiry] button, select charging personnel(double-click) and save

Q2. Where can I apply for the reservation for a visit?

A visit to the Namyang Research Center is made through the application of reservation by the visitor and the approval by the team that the visitor intends to visit (the person in charge of the field team).

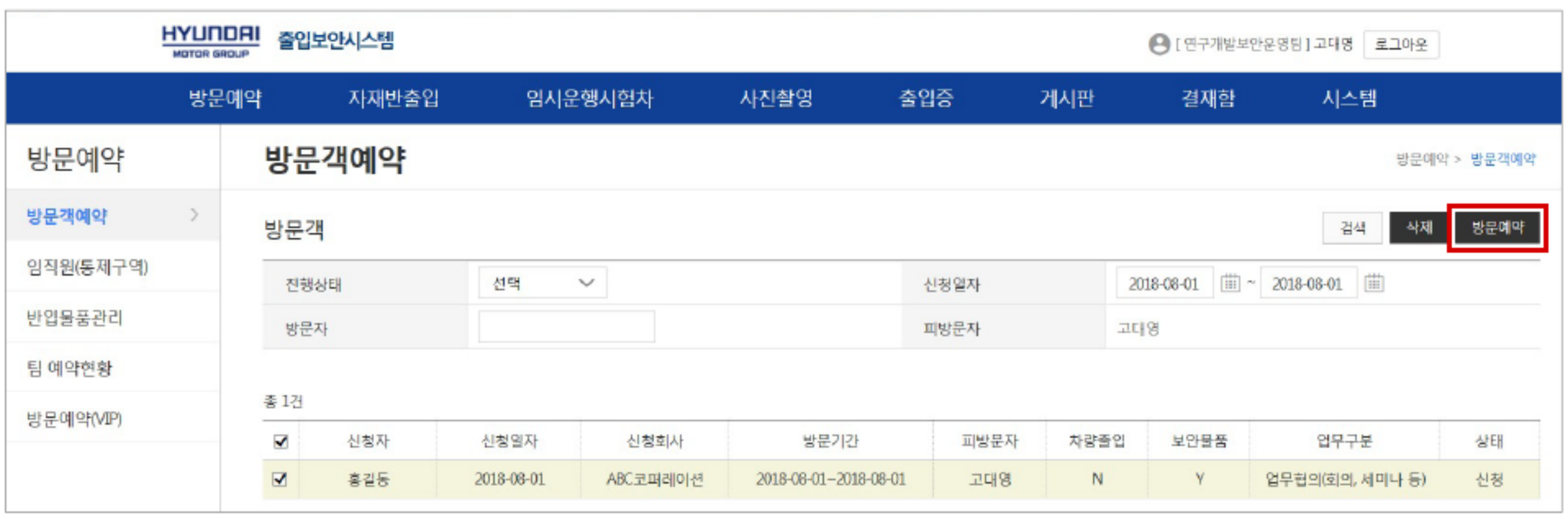
1. Application for a visit (visitor):

Visitors can access the Access Reservation System (visit.hmc.co.kr) in advance, enter visitor information, and apply for a visit.

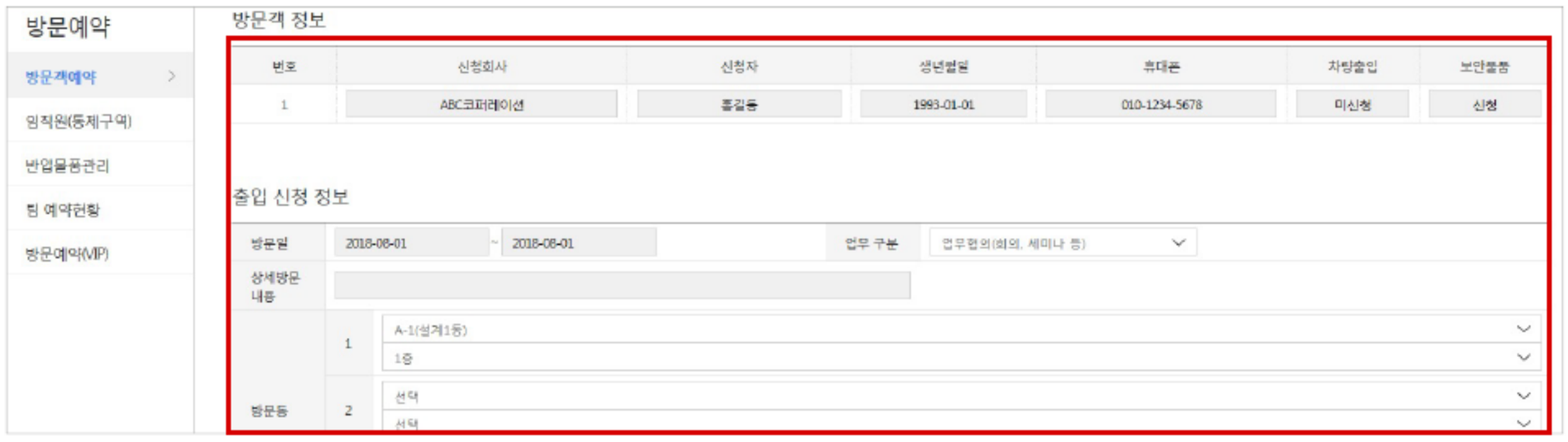


2. Approval of a visit (person whom the visitor intends to visit, the person in charge of the field team)

① After accessing the Namyang Access Security System Visitor Reservation site, click ‘Reserve a visit’ in the top right corner.



② After confirming the date of visit, division of work, and the building to be visited, submit for approval.



How to Install the Mobile Namyang Access Security System

How to install the mobile app

Detailed installation manual can be found in Namyang Access Security System Notice

STEP 1
Go to https://goo.gl/6p123j

STEP 2
Select the applicable OS (Android, IOS)

STEP 3
Click the downloaded file

STEP 4
Click the Install button

If the installation file is downloaded as a .zip file, do not unzip the file.
Change the filename extension to .apk and install the file.

02 모바일 남양출입보안시스템

일반 기능

❶ 방문신청 현황

방문예약 상신 및
상신 건의 진행상태 확인

❷ 내가 결재할 문서

방문예약, 자재반출입, 임시운행시험차,
사진촬영의 결재 진행

❸ 공지사항 & FAQ

남양출입보안시스템과 관련된
공지 등을 확인

보조 기능

❶ 보안 승인

방문객이 반입한 물품의 반출을 승인

❷ 결재 진행 상태 확인

진행 중인 결재 건의 상태 및 결재자 확인

How to apply for a visit through mobile devices

(Website address - https://visit.hmc.co.kr)

1. Apply for a visit to the person in charge of the field team for a meeting or a seminar.
2. View the progress of my reserved visit.
3. Check announcements related to a visit.

Photographing Procedure

- The entire Namyang Research Center is a secure area, and unauthorized photographing using personal cell phones and cameras is prohibited.
- If it is necessary for business purposes, photographing must be carried out according to the procedure set forth below through prior application.

STEP 1
Apply for photographing

STEP 2
Approve

STEP 3
Receive the photographing armband.

STEP 4
Carry out photographing

STEP 5
Security review for photographing

STEP 6
Return the photographing armband

Classification	Apply for photographing	Approve	Collect the photographing armband.	Security review	Note
Research institute Employee	Namyang Access Security System	Photographing target Team in charge	Use of each team's armband	Photographing target Team in charge or Research Information Protection Team	In case of photographing without permission, Personnel disadvantages will be imposed in accordance with security regulations.
Employees working in other areas			Front/Rear gate		
Visitors	Visit Reservation Website (Application for bringing in a camera is required)		Front gate		In case of violation of regulations, photos taken will be deleted and access to the research institute will be permanently suspended

※ In principle, photos should be taken by an employee of the research institute, but if photographing using special equipment is required, it can be done by sending a official letter

FAQ

Q1. What is the procedure for photographing and data transmission by outsiders?

① Apply for access by the visitor : Register and report camera and bring-in articles

② Carry out photographing : Accompaniment by an executive or staff member and wearing of the photographing armband are required.

③ Approval procedure for bringing out articles : Security review by the bring-in article approval team

④ Bring out and send data : - An e-mail can be sent upon the approval from the team manager (Bring In Article Approval Team).

Temporary camouflage cover removal procedure for new cars

Information on the procedure to remove the temporary camouflage cover for a new vehicle is provided as follows in case it is necessary to release the security of a new car for vehicle performance test, local service evaluation, early mass production, advertisement filming, new car exhibition event, etc. (Target vehicle: 'When camouflage covering and taping are not applied' or 'When taping without foam is applied alone')

Apply by submitting the official letter form including the following items.

※ Cooperation team: Hyundai Information Protection Center (Hyundai/Genesis models), Kia Information Protection Center (Kia models), R&D Information Security Team (common)

① Vehicle consignment and local evaluation schedule/place

② VIN.NO of vehicle to be evaluated

③ Reason for temporary security release request

④ (If necessary for business purposes) Contents and reason for cutting the camouflage cover in specific areas

(front and rear sensors, radiator grill, etc.) according to the evaluation characteristics

⑤ Fill out and attach an application for temporary camouflage cover removal for a new car (The form can be downloaded from

Namyang Access Security System>message board>Announcements>No. 31 article)

Matters to be observed

① Remove the camouflage cover or apply taping without foam only to the target vehicle during the period

② Apply the camouflage cover to the vehicle when moving between controlled areas and consigning the vehicle

③ Prohibit the removal of camouflage cover in the area adjacent to the ceremony or an event with outsiders

④ Camouflage covering (interior/exterior and locking device) or complete camouflage covering (vehicle body cover) measures when the driver is absent while taking the vehicle outside of the company

Others

- Temporary security release upon self-judgment without notice of temporary security release during testing/evaluation in secure areas such as driving test centers, workshops, chambers, and Seosan straight road in Namyang Research Institute where the security environment (card reader, CCTV, vehicle blocker, etc.) is configured (needs to comply with item No. 3 above)

- Consult Hyundai/Kia Information Security Center and R&D Information Security Team for other special matters (needs to comply with item No. 3 above)

- Refer to New Vehicle Security Management Regulations (HR-IS-BA-002)

What is the procedure for vehicles to access the research institute?

Due to the nature of tasks, there are always many cars and not enough parking spaces.
Therefore, we ask all our executives and staff members to observe the vehicle access procedure.

Classification		Access procedure	Note
Executives and staff members (working in the research institute)	Team manager or higher positions	Access after having the team managers or higher levels's vehicle sticker and computer system registration confirmed	Refer to 'Vehicle sticker issuance procedure for executives and staff members'
	Employee (personal vehicle)	Access after having the employee's vehicle sticker and computer system registration confirmed (it is possible to pass the gate before and after business hours)	
	Test vehicle	After application for temporary driving of the test vehicle is approved, have your license plate number checked and tag your employee ID card when entering the gate.	Apply at Namyang Access Security System 'Temporarily Operated Test Vehicle' · Can apply for up to 3 months · Decision by the team manager
	Vehicles for business purposes	Access after having the sticker for vehicles for business purposes confirmed	Limited to vehicles under the name of Hyundai Motor Company
Executives and staff members (working in other areas)	Executives or higher levels	Access after presenting their business card to security personnel	
	Employee (personal vehicle)	Use the parking lot at the front gate, use a shuttle bus inside the research institute	
	Vehicles for business purposes	Entry into the gate is possible	Limited to the general affairs team's vehicles for business purposes (confirm the vehicle sticker)
Outside visitors	Visitors	Use the parking lot at the front gate, use a shuttle bus inside the research institute	
	VIP	Apply for vehicle access when reserving for a visit (A matter of arbitrary decision by the department head)	Refer to 'Access procedure for visitors'.
Subcontractor	Delivery/construction company's vehicle	Apply for vehicle access when reserving for a visit (A matter of arbitrary decision by the team leader)	

FAQ

Q1. Is it possible to issue a vehicle access pass for construction/supply/service company vehicles?

If the issuance requirements are met, it can be reviewed and issued after application.

Issuance requirements

① Vehicles of construction/supply/service companies continuously working on site (issuance is not allowed for all other vehicles)
② Vehicles accessing for more than 1 month
③ Driver get the advance issuance of an access pass (or application for reservation for a visit)

How to apply

: The field manager applies at Autoway - My Tasks - Access Namyang Access Security System – Access Pass – Contractor's Employees/ Vehicles (Registration of vehicle security pledge is required, Download the form from Namyang Access Security System – Security Forms)

Q2. What if a visitor's vehicle (other than VIP) needs to gain access to the premises?

Access is not allowed for the purpose of transporting people, and you must use the general parking lot at the front gate and use the shuttle bus within the premises. If access is unavoidable for any other reason, it is necessary to consult with the person incharge of the R&D Information Protection Team.

Q3. Can other company's brand vehicles also can access the research institute?

Other company's brand vehicles are not allowed for access. If access is required for unavoidable reasons,
a separate request must be made by e-mail to the person in charge of the R&D Information Protection Team.
(Reason, date of visit, affiliation of visitor, name of visitor, date of birth, license plate number, vehicle type)

Q4. I need to have a test vehicle located outside of the research institute come into the research institute. What should I do?

① When an outsider brings a test vehicle: Visit visitor reservation (http://visit.hmc.co.kr)
※Refer to the 'Visitor Access Procedure' manual
② If an executive or staff member brings a test vehicle: Apply at Namyang Access Security System - Reservation for Visit - Executives and Staff Members (restricted areas) (prepare based on the driver who entered the gate initially)
③ At the time of entering the gate, check for the reservation for a visit and place the stamped printed document on the vehicle.
④ Submit a stamped printed document at the time of exit

Sticker issuance procedure for vehicles owned by executives and staff members

For team managers or higher levels, access to the research institute by own vehicle is possible through the application for a vehicle sticker and pre-registration, and for employees, they can gain access to the research institute using their own vehicle before and after business hours only through the application for issuance of a vehicle sticker.

How to apply for a vehicle sticker by team managers or higher levels

Target persons for issuance	Team managers or higher levels affiliated with R&D headquarters and working in Namyang Research Institute
Contents	Access through the front and rear gates and parking inside the Research Institute available at all times
How to apply	① Visit the person in charge within the R&D Information Protection Team (applicable on instead): Check the team name, person's name, and license plate number ② Confirm the employee and issue the sticker immediately
Vehicle replacement	① Check the license plate number of a new vehicle and visit the person in charge within the R&D Information Protection Team - Return the previously issued vehicle sticker
Vehicle repair	Apply to the person in charge within the R&D Information Protection Team by e-mail (write the reason, license plate number and period)
Reference	Only one sticker is issued for one person (only one vehicle can be registered for each person)

How to apply for a vehicle sticker by employees

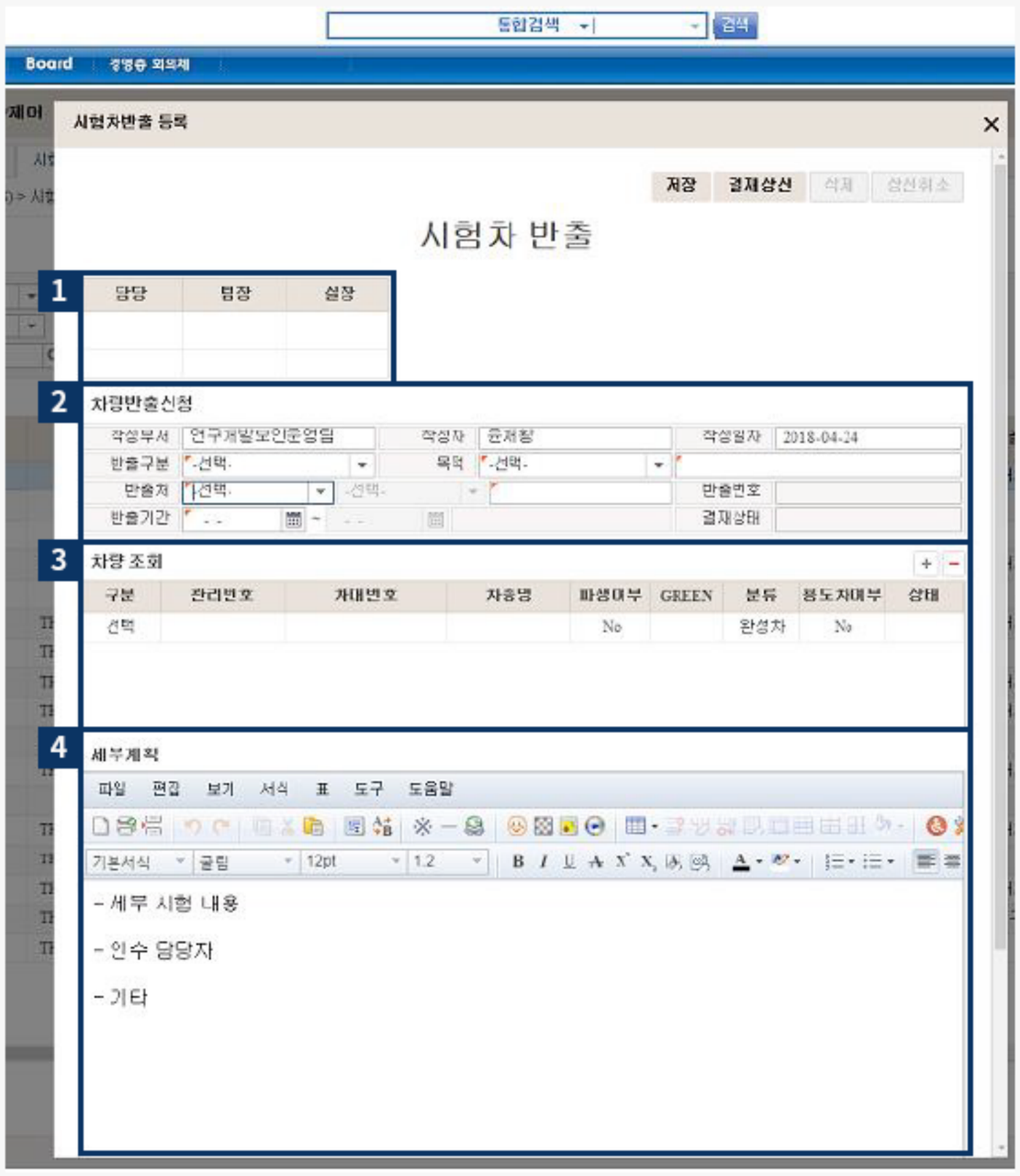
Target employees for issuance	Team members working in the research institute
Contents	Access is allowed for the purpose of passing through the premises during commuting time (A penalty applies for delays of more than 30 minutes) ♧ Penalty for vehicles parked inside of the premises after entering the gate with the purpose of passing through the premises - Crackdown for the first time: Send an e-mail for guiding the exit - Crackdown for the second time: Recovery of the vehicle sticker (no re-issuance for 6 months) - Crackdown for the third time: Recovery of the vehicle sticker (no re-issuance for 1 year) On-site parking available before and after business hours (weekdays before 08:00 and after 17:00, on weekends)
How to apply	① Apply at Namyang Access Security System – Access card – Vehicle registration ② Receive the mail bag (It takes up to 7 days)
Vehicle repair/replacement	① Click the expiration process at the top right side of Namyang Access Security System – Access Card – Vehicle Registration and re-apply for the vehicle sticker at Vehicle Registration
Reference	Two stickers are issued for one person (Two vehicles per person can be registered)

Test Vehicle Bring-out Procedure

- When it is necessary to bring a test vehicle out to our other business sites or a partner company for the purpose of test evaluation and service performance, follow the procedure below.

Procedure to apply for bringing out the test vehicle

Select Autoway > AutoONE > Vehicle Management System > Bring out test vehicle



1 Apply for bringing out the vehicle
- Enter the bring-out category, purpose, place to bring out and period of bring out

2 Inquire about vehicle
- A vehicle registered on the Vehicle Management System : Select 『Inquiry』
- A vehicle not registered on the Vehicle Management System : Select 『Enter directly』

※ When entering directly, write vehicle information in detail

※ Status of Vehicle for a Certain Purpose : Enter “Yes”

3 Add and delete rows
Use the +/- button to add or delete bring-out vehicles

4 ④ Detailed plan
- Specific test details
- Person in charge of take over: The person who receives the vehicle
- If any other explanation is required

5 ⑤ Regulation regarding arbitrary decision
- Re-bring in/free bring-out of test vehicle : arbitrary decision by the team manager
(Other areas in our company : arbitrary decision by the team manager)
- Re-bring in/free bring-out of BIW : arbitrary decision by the team manager

※ When bringing out a vehicle whose security has not been released to a company, an additional security pledge is required to provide a test vehicle in addition to the bring-out certificate.

FAQ

Q1. Who should I choose as the arbitrary decision maker when I fill out the test vehicle bring-out certificate?

1. Select the arbitrary decision maker shown below for the test vehicle according to the bring-out type.

Classification	Apply for bring-out	Right to make an arbitrary decision	
		Procedure for bringing in/out of general articles again	Free bring-out
Test Vehicle	Vehicle Management System	Team manager	
BIW			
Main parts	Namyang Access Security System	Team manager	
Regular parts			

Issuance of a temporary vehicle pass for an injured employee

A temporary vehicle pass is issued to injured/sick/handicapped employees in order to allow them to commute using their personal vehicle.

Issuance of a temporary vehicle pass for injured/sick/handicapped employees

Target employees for issuance	Injured/sick/handicapped employees working in the research institute	
How to apply	Handicapped employees	Apply by e-mail (for up to 1 year) ※ Attach a copy of the handicapped parking sticker E-mail recipients: Team manager of the R&D Information Protection Team, team manager of the field team, and person in charge of access pass issuance
	Injured/sick employees	Apply by e-mail (for up to 3 months) ※ If you apply for an access pass for more than 1 month, attach a medical certificate issued within 2 weeks from the date of application. E-mail recipients: Team manager of the R&D Information Protection Team, team manager of the field team, and person in charge of access pass issuance
Employee Vehicle repair/replacement	Apply to the person in charge of the R&D Information Protection by e-mail	

How can a visitor make a reservation?

Visitors who visit the research institute for the first time are all Hyundai Kia Motors' customers.
Proper prior understanding and guidance on our strict access security procedures are necessary to prevent any inconvenience during their visits.

'Access procedure for visitors'

STEP 1

Outside visitors apply for reservatiotn directly on the online website.
https://visit.hmc.co.kr

STEP 2

The person whom the visitor intends to meet (an employee of the research institute) approves the application at Namyang Access Security System.

STEP 3

The visitor accesses through the front gate (All visitors should access through the front gate in principle)

※ A security sticker should be attached to all camera phones.

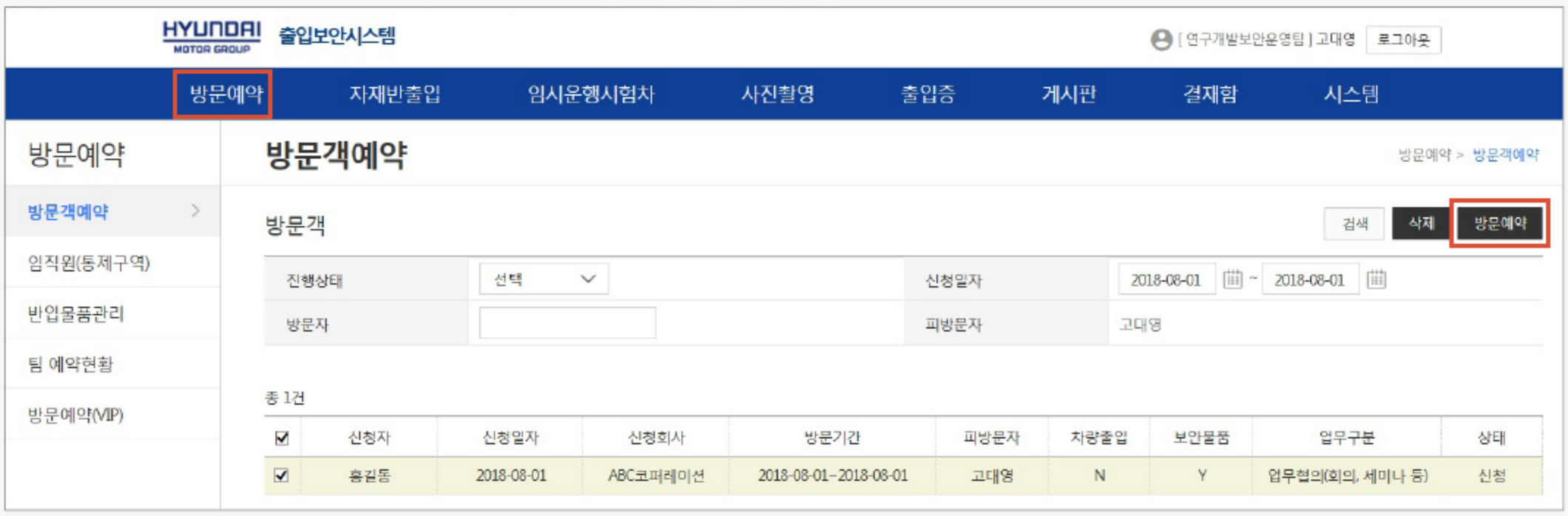
'Procedure to apply for an access reservation by visitors'

1 **Outside visitors apply for a visit on the Access Reservation website in advance.**

Website address for the access reservation by visitors: https://visit.hmc.co.kr

2 Approval by the person whom the visitor intends to meet (a staff member of the research institute):

Access Namyang Access Security System → Click 'Reservation for Visit' in the top right corner → Check the contents and approv



3 Visitors access through the front gate (with the security sticker attached to the mobile phone)

※ Arbitrary decision standards for each visitor access condition

Conditions	Arbitrary decision standard
Meeting room outside the building and on the 1st floor	Person in charge (Arbitrary decision by the team manager when bringing in security items)
Office/Site	Head of the division

When using a visitor’s vehicle

: Outside visitors' vehicles should use the parking lot at the front gate and move inside the research institute using a shuttle bus.

However, in the case of delivery/construction/test and VIP vehicles, it is possible to apply for access into the research institute.

(Enter visitor information on the vehicle registration column when applying for reservation for a visit)

※ Arbitrary decision standard

Conditions	Arbitrary decision standard
VIP vehicle	Director of the Center/Head of business department
Delivery/construction/test vehicle	Team manager

When a visitor needs to bring in security items (photographing/storage devices, etc.)

1 Register and enter bring-in articles in the visitor information column when applying for reservation for a visit

2 Register and enter bring-in articles in the visitor information column when applying for reservation for a visit
The person whom the visitor intends to meet (an employee of the research institute) approves the application at Namyang Access Security System.

Visitor's laptop computer bring-in procedure

STEP 1
Write security devices in the application column when applying for reservation for a visit
(If using a port, select the port to be used)

STEP 2
The person whom the visitor intends to meet
(an employee of the research institute) approves the application at Namyang Access Security System.

STEP 3
Have your application record checked at the front gate and install the security program

STEP 4
The person whom the visitor intends to meet
(an employee of the research institute) approves the bring-out of the articles that were brought in at Namyang Access Security System when exiting the gate.

※ In case of brining out data or if the security sticker is removed, it is approved by the team manager
(All other issues are approved by the person in charge)

FAQ

Q1. If an employee who is not an Research Institute employee needs to accompany visitors and access the premises,

The visitor can gain access after applying for a visit and receiving the approval from the team residing in the research institute.
However, if the team residing in the research institute is absent, contact the R&D Information Protection Team.

Q2. If the security sticker is removed from the laptop computer after entering the gate?

If the sealed security sticker is removed from the laptop computer for reasons such as the use of the port after entering the gate, a statement of reason for port use must be written when applying for bring-out on the Namyang Access Security System.
(A matter of arbitrary decision by the team manager)

Q3. Can visitors enter through the back gate?

All visitors should enter and exit through the front gate.
However, only visitors using the shuttle bus or public transportation (bus No. 22) can enter through the rear gate. However, the visitors who entered through the rear gate should exit through the rear gate, and the visitors who entered through the front gate should exit through the front gate.

Q4. What should I do if a place to visit is added after entering the gate?

You will need to make an appointment for a visit and obtain approval again.
(You can also make an appointment through the visitor's mobile phone (https://visit.hmc.co.kr)
After obtaining approval, you can let the information desk in each building know.

Q5. Can Namyang employee apply for reservation for a visit on behalf of me?

It is impossible. When applying for a visit, consent is required for the provision of personal information (date of birth/mobile phone number, etc.), so our employee cannot go through the procedure on behalf of someone.

Access procedure for weekend visitors

Procedure of a visit during the weekend

Classification	Access location	Access procedure
Health club/swimming pool	Rear gate	Have your employee ID card and the membership card confirmed by the UT checkpoint (next to the affiliated hospital) and write the access ledger (Move inside of the research institute on foot)
History Hall/Gym	Front gate	Enter into the gate after submitting your employee ID card and recording on the ledger ※ If the access using your private vehicle is necessary, have your employee vehicle sticker confirmed (How to apply for an employee vehicle sticker: Check 'Sticker issuance procedure for vehicles owned by executives and staff members'.)
All other reasons		No access is allowed in principle.

FAQ

Q1. Can I bring my family into the research institute using my own vehicle during weekends?

You can enter in the front gate after submitting your employee ID card,
but you cannot enter into the rear gate using your own vehicle. (Park your vehicle and enter the gate)
(However, the vehicle sticker must be attached)

What is the research institute access procedure for a partner company's employee?

In order for a partner company's employee to access the research center for technical services, he/she must make a reservation for a visit and obtain a temporary access pass at the front gate.
(However, issuance of a long-term access pass is possible for a partner company's employee who is resident and working on site.
Refer to "Access pass issuance procedure for other company employees working inside the institute".

Access procedure for a partner company's employee for technical service

STEP 1

The partner company's employee should apply for reservation directly on the online site.
http://visit.hmc.co.kr

STEP 2

The person whom the visitor intends to meet (an employee of the institute) approves the application at Namyang Access Security System.

STEP 3

The visitor accesses through the front gate (All visitors should access through the front gate in principle)

※ You can apply for a maximum of 1 month as the period of visit by each application.

FAQ

Q1. Can partner company’s and GE employees apply for the issuance of a long-term access pass?

- Partner company's employee: Issuance of a long-term access pass is available for a partner company's employee who is resident on site or who does not reside on site but accesses for more than 2 weeks/month (up to 1 year).
- GE employee: When a GE employee applies for a long-term access pass on AutoONE, the R&D Quality Assurance Team reviews the application and issues a long-term access pass (up to 1 year)

Visitor's laptop security approval procedure

If a visitor who accesses the Namyang Research Institute wishes to bring in his/her computer equipment that can save data, an advanced approval procedure according to the following steps is necessary when reserving for a visit. (Target equipment: laptop computer, tablet PC, external HDD, USB, etc.)

1. Advanced registration (visitor)

1 ① Access to the Access Reservation System (http://visit.hmc.co.kr)

2 Click Register Bring-in devices on the visitor's information column.

3 Register and enter bring-in security articles (period of use, purpose, item name, quantity, serial No, etc.)

2. Approval of reservation (person whom the visitor intends to meet / Namyang employee)

1 After accessing the Namyang Access Security System Visitor Reservation site, click ‘Reserve a visit’ in the top right corner.

2 After confirming the visitor's security item application information, click Approve.

자주 묻는 질문

Q1. What is the procedure for bringing out the visitor's laptop computer after using it?

1. After connecting to Namyang Access Security System > Reservation for Visit, click "Manage bring-in articles' on the left menu.

2. Click 'Bring-out' from bring-out approval items at the bottom right side.

3. Enter whether to bring out saved data or not, write the name of file to bring out, etc. enter the number of removable security stickers, and click Approve.

※ When it is necessary to bring out saved data, the team manager's approval is required (once within the entire period of visit)

Access Procedure for Uiwang Research Institute

Access location	Classification	Contents	Note
Access through the front gate/ the west gate	Outside visitors	Apply for a visit in advance at https://visituw.hyundai.com/ (Requires the input of visitor information)	Access procedure for the front and west gates
		Access after exchanging the access pass in the visitor center	
	Employees from other regions	Access after having the integrated employee ID card verified at the enterance gate	
Access to the research building	Outside visitors	Access after exchanging your access with the research building access pass at the information desk on the first floor of the relevant building - Only access permission to the pre-reserved floor is granted.	Access procedure for restricted areas
	Employees from other regions	Access after exchanging your access with the research building access pass at the information desk on the first floor of the relevant building - A separate access reservation is required when visiting the floor of another affiliate.	

Restricted areas and how to apply for access permission

Q1. Where can I apply for access permission to restricted areas where access is not allowed?

Apply for access permission in the ‘Employee ID Card Management System at Autoway - My Tasks
- After applying for access permission, access permission is granted only after it is approved by the team in charge of restricted areas.

Q2. How do I set the reader device permission so that only certain employees can access?

Make a request to the person in charge of the R&D Information Protection Team by e-mail
(Preparation of the form is required: Reader device No. and status of restricted people for access, etc.)
: If you are assigned to the team in charge of the reader devices managing, you should accept other employee’s access permission request from the employee ID card management system.
※ The main entrance gate and normal offices are not permitted (excluding design buildings and PDI building)

What is the procedure for employees working in other areas to access the research institute?

Namyang Research Center Access procedure for Employees Working in Other Areas

After submitting your employee ID card at the information desk in each building, receive a temporary pass and access.

※ However, when visiting the Design Building, PDI 1-3 Buildings, or Quality Assurance Building, apply for the reservation for a visit in advance through the Namyang Access Security System (A matter of arbitrary decision by the team manager of the team that the visitor intends to visit)

FAQ

Q1. Is it possible to issue a long-term access pass if an employee of other headquarters working in other areas accesses the Namyang Research Center periodically?

It can be issued only to employees who meet the requirements. Because the access pass is issued very strictly for security reasons,
please understand that if the following requirements are not met, the access pass will not be issued.

※ However, in the case of executives, the access pass can be issued regardless of the requirements.

- Issuance Requirements: At least 10 days of access history in the previous month or 120 times a year
- How to apply:

① Apply by submitting the official letter (state the visitor's team / employee ID number / name / place of work / reason for application)

② Confirm issuance requirements

③ Visit and collect an access pass issued

Access Procedure for Security Areas in the Research Institute

Access procedure for restricted areas in the institute by executives and staff members

Design building

All executives and staff members should obtain access through the reservation procedure for a visit using the Namyang Access Security System. (A matter of arbitrary decision by the team manager of the visitor)

PDI1~3 buildings, quality assurance building

Executives and staff members working in other areas should obtain access through the reservation procedure for a visit using the Namyang Access Security System. (A matter of arbitrary decision by the team manager of the visitor, attachment of a security sticker to a personal mobile phone)

※ No separate procedure is required for executives and staff members of Namyang and Mabuk Research Institutes.

※ Dress code when accessing the line: Research Institute uniform (for permanently stationed executives and staff members of the Research Institute), vest for outsiders (other areas / provided by the front desk)

What is the access procedure for staff members employed locally by the overseas research institute?

Access application procedure for staff members employed locally by the overseas research institute

STEP 1

Application by the person in charge of the research institute using the official letter

STEP 2

Approval of the official letter by R&D Information Protection Team

STEP 3

Confirmation of the relevant staff member at the front gate and issuance of a temporary pass

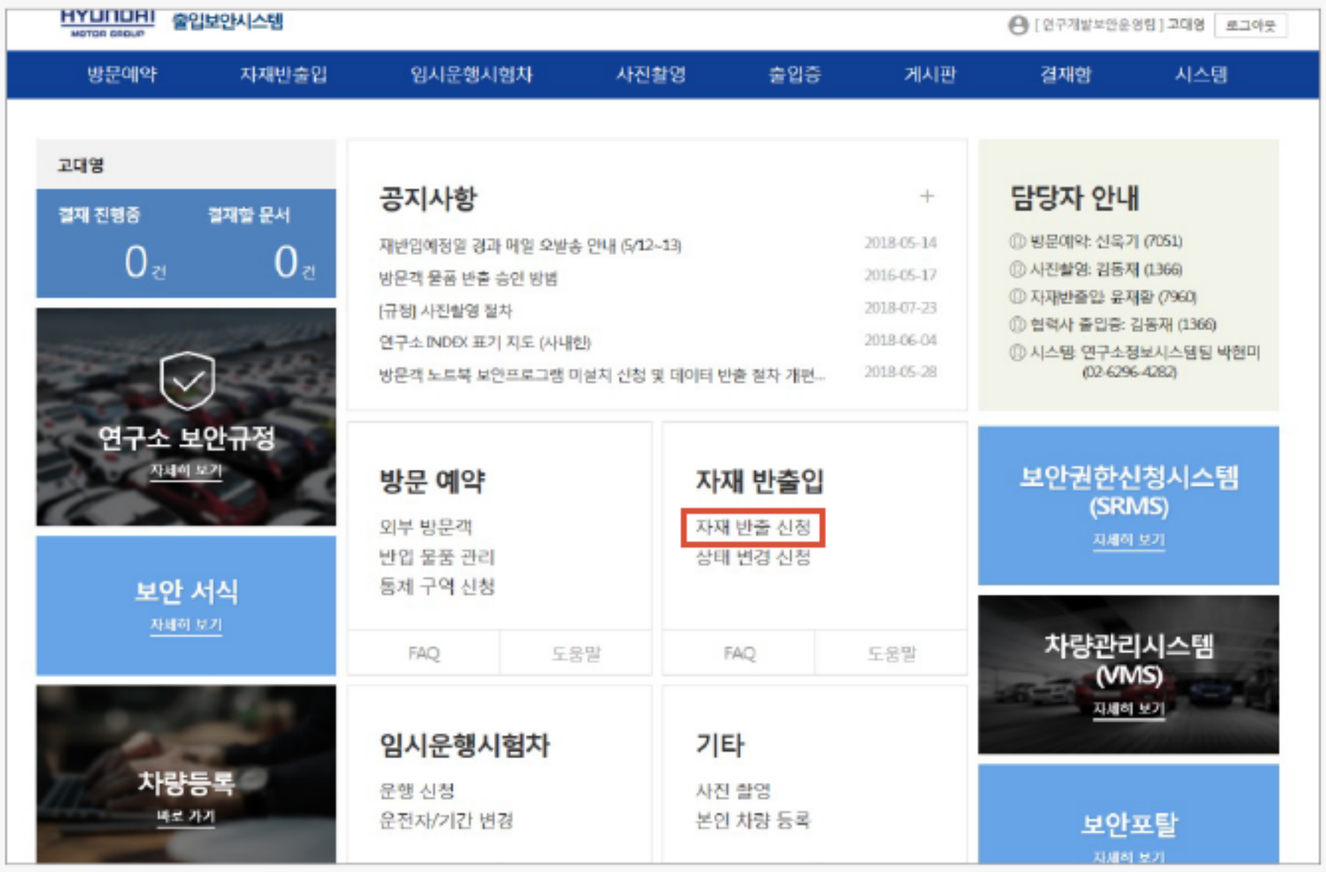
- Contents of the official letter form: Visitor's team / company ID number / name / place of work / reason for application / period of visit
- Designation of a cooperation office if the place of visit is included in the restricted area
  - PDI1~3 Buildings / Total Quality Assurance Building: Pilot Planning & Support Team
  - Hyundai Design Building: Hyundai Design Program Team
  - Kia Design Building: Kia Design Planning Team

Re-bring-in/out procedure for general articles

Except for computer equipment such as vehicle parts, test equipment, and tools, all institute goods are brought in and out according to the procedure below.

1. Application for bring-out in advance

1 After accessing Autoway > My Menu > Namyang Access Security System, click Apply for Material Bring-out



2 After entering and saving general items, click Approve.

1	Classification of bring-out: Select among charged/free/re-bring-in/out	5	Enter the person who brings out: Enter the name of actual person who brings out through the front/rear gate
2	Enter the purpose of bring-out	6	Enter the scheduled date of re-bring-in
3	Select bring-out method: Our vehicles, our personnel, partner company's vehicles, partner company's employees Parcel service, others	7	If it is necessary to bring in and out frequently during the period, enter official letter No. for the grounds.
4	Enter the place to bring out : Our company in other areas, domestic/overseas partner companies	8	Enter information on goodss to be brought out - Enter "-" if there is no control No. (Control No. is a required item and the bring-out certificate cannot be filled out if it is not entered.) - Write No. in the Remarks column for easy identification. (ex. Computer S/N, Part No., etc.)

2. Bring-out Procedure

After printing out the bring-out certificate, carry the articles and have them checked at the front gate and bring out the articles (by the person who brings out). (Possible to print the bring-out certificate out at the front gate if not printed out)

① Charged/Free bring-out: Print out one bring-out certificate and submit it to the information desk at the front gate.
② Re-bring-in/out: After printing out two bring-out certificates, submit one to the information desk at the front gate, have the other certificate stamped for confirmation by the information desk at the front gate, and submit it when bringing in.

FAQ

Q1. How can I differentiate between charged bring-out, free bring-out, and re-bring-in/out?

1. You can select the type of bring-out according to the following information.

Classification	Definition
Charged bring-out	In the case of bringing out articles on condition that the price for such articles is received (Cooperation from the finance team is necessary)
Free bring-out	In the case of bringing out articles on condition that the price for such articles is not received
Re-bring in/out	In case goods that were brought out from the institute are brought into the institute again

※ Bring-out Procedure by Type

	Free bring-out	Charged bring-out	Re-bring in/out
Team from where articles will be brought out	Fill out the bring-out certificate on Namyang Access Security/Vehicle Management System → Print out after approval is received…>…… ※ If car dispatching is necessary, apply at the General Affairs Support Center		
R&D Finance Team		R&D Finance Team Confirmation: After confirming receipt of the payment to our company, key-in	
Front gate	Check the system and actual articles → Exit the gate		

Q2. In case the bring-out date I entered when filling out the bring-in certificate has passed, how should I bring out?

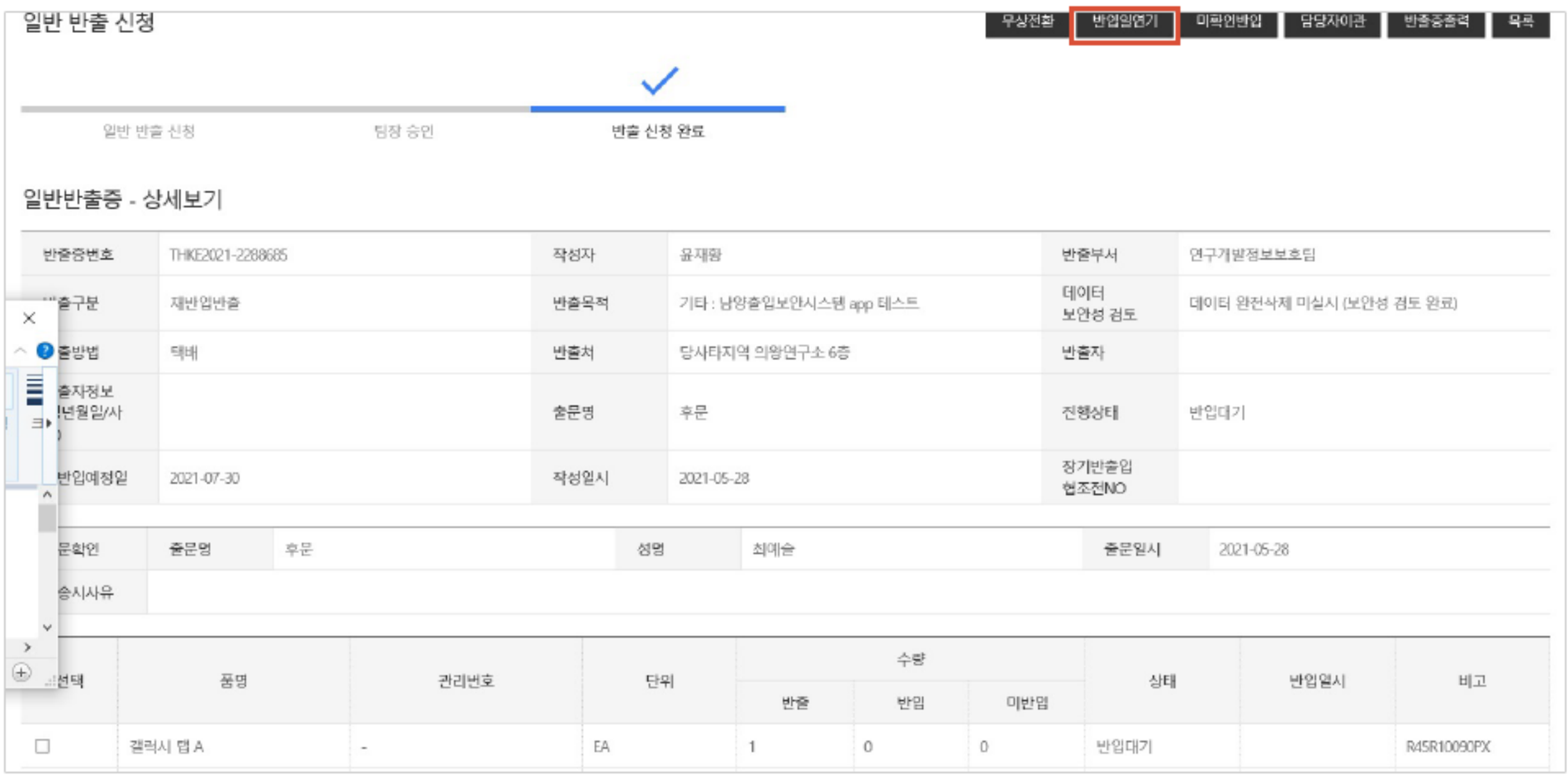
Even if the bring-out date has passed, you can bring out if you have the bring-out certificate you prepared.

Q3. What should I do if a bring-out article has no control No.?

Control No. is a required item and the bring-out certificate cannot be filled out if it is not entered.
Enter "-" if there is no control No. and skip it.

Q4. What should I do if the expected re-bring in date has passed?

If the expected re-bring in date you entered when filling out the bring-out certificate has passed,
you can write the reason for the postponement through the system and receive approval from the team manager.



Q5. How can I send a package by parcel service?

Follow the procedure below for sending a mail item or a package to the outside by parcel service from the research institute.

Classification		Reception route	Required documents	Send to	Note
Mail bag		Document receipt and sending office	-	In-office mail box	
Letters to be sent outside the company	Registered mail	Document receipt and sending office	-	- Visit the document receipt and sending office and submit an application	- Free bring out certificate is not required - Only registered mail & door-to-door reception are possible when using the Document receipt and sending room - The price varies by registration level
	Registered mail Parcel	R&D) General Affairs Team	1. Captured approval completed screen of the business lounge 2. Free bring out certificate (Limited to parcels)	- In-office mail box ※ Put together with required documents (half-packaged for the parcel)	- Separate application for mail is required at the business lounge ※ Applicant>Team Manager > Approval by the person in charge - Personal mail cannot be sent - A security officer visits the document delivery room and checks the contents and bring-out certificate.
Parcels to be sent outside the company	Payment on delivery	Document receipt and sending room	Free bring out certificate	- In-office mail box ※ Put together with required documents in half -packaged state	- A security officer visits the document delivery room and checks the contents and bring-out certificate.
	Prepayment			- Visit the document receipt and sending office and submit an application ※ Put Free bring out certificate together with equired documents in half-packaged state	- Submit an application with the delivery fee in cash together to the document receipt and sending office (The cost in cash will be collected by the parcel company) - UT/C checkpoint checks the contents, submits the bring-out certificate and stamp the box.

Procedures for bringing in/out of computer equipment

Procedure for bringing in computer equipment for business purposes to the Namyang Research Institute

Classification		Access procedure
Laptop computers and mobile storage devices	Research institute's employee	Apply for bringing-out and bringing-in on the Namyang Access Security System
	Employees of companies other than the research institute	Fill out the confirmation document for bringing in articles or Reserve a visit on the Namyang Access Security System ※ Application for use is required when using the network for the first time (Security Permission Application System)
Photographing equipment	Research institute's employee	1) Company assets: Apply for bringing-out on the Namyang Access Security System 2) External assets (brought in by the visitor) : Apply electronically on the Visit Reservation system 3) External assets (brought in by executive or a staff member) : Consult the R&D Information Protection Team in advance
	Employees of companies other than the research institute	Consult the R&D Information Protection Team in advance

FAQ

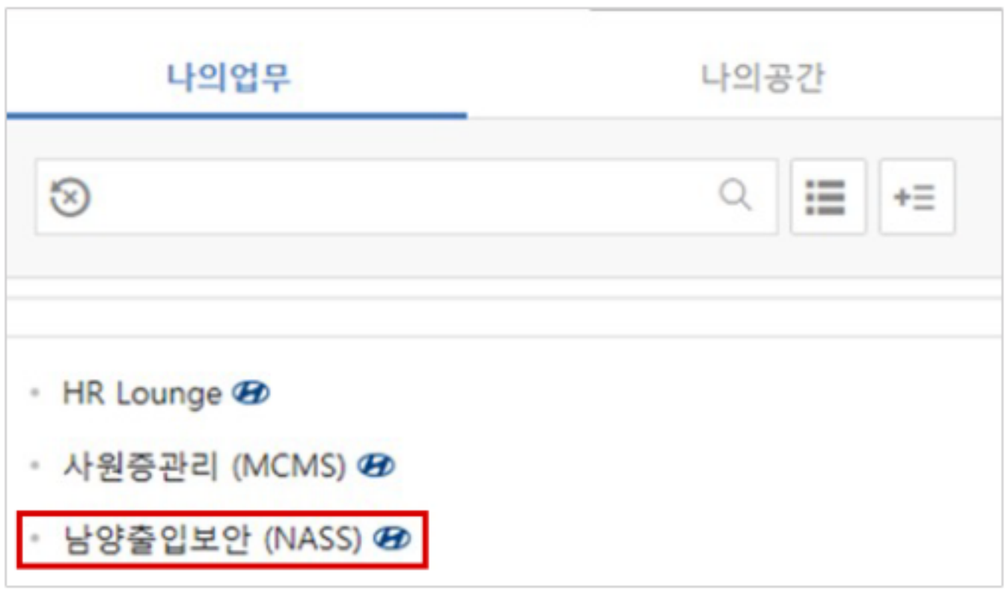
Q1. What is the procedure for bringing out/in a laptop computer for business purposes?

Re-bringing in/out of laptop computer

If you need to bring out your laptop computer for business trips to other areas, tests/evaluations, etc.,
you must apply for re-bringing out the laptop.
Equipment can be brought in/out according to the Namyang Access Security System re-bringing in/out procedure.

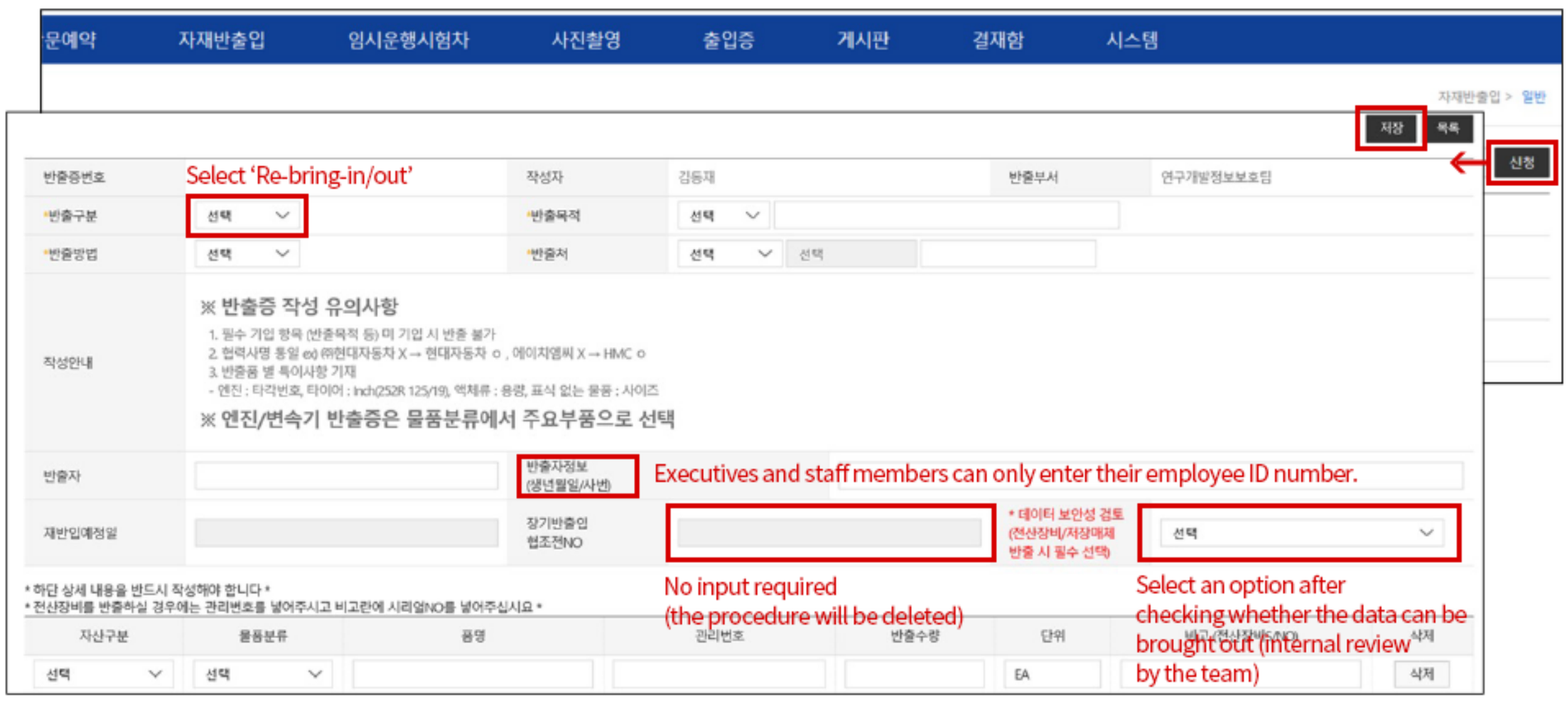
1. Autoway - My Tasks > Access Namyang Access Security System (Common for Namyang/Mabuk/Samsung)

※ Uiwang: Uiwang Access Security System > Bring-out Articles > Apply for Bring-out



2. Re-bringing in/out > General > Click Apply

- Fill out each input column, save and submit for approval.



3. After approval within the team is granted, re-bring in/out laptop computer
(Frequent re-bringing in/out during the period is possible)

- If you bring a printed copy of the bring-out certificate, you can carry out the bring-in and bring-out procedures smoothly.

※ Place to go through the laptop computer bring-out procedure

1) Front/Rear gate

2) Information desk on the main buildings
Target : Design 1/2 Building(A-1, A-3) , PDI 1/2/3 Building, Hyundai/Kia Design Building, Commercial Design Building,
PT Environmental Precedent Research Building

※ Go through the procedure at the main information desk on the 1st floor in all workplaces except for Namyang Research Institute.

Q2. Is there a procedure for bringing in computer equipment into the premises on a long term basis by an outside partner company?

<Long-term bring-in procedure for laptop computer/computer equipment by partner companies>

1. Apply for bringing in computer equipment through reservation for a visit.

2. Process 'delivery' of the relevant item in the 'Namyang Access Security System > Manage Bring-in Articles' menu

※ Frequent re-bring-in/out within the bring-in period is not allowed.

<Temporary Account/Computer Equipment Registration Procedure>

↑ Normal policy can be applied only when the registration is carried out after the equipment is brought in.

1. Security Permission Application System 1-1 Application for Security Program Account (AD/DRM)

(Path: Autoway > My Tasks > Security Permission Application System)

2. Security Permission Application System 2-2 Application for Cancelation of Unauthorized Computer Equipment

※ After completing the application, please follow the instructions for self-installation of the security program shown when connecting to the Internet (Inquiry: Help Desk 02-801-4321 - 1 Security Operation Center)

<Equipment and data management precautions>

1. Data type to be used (utilization of test data, utilization of actual work data, etc.) and how to move work data

→ Utilization of test data: Allowed

→ Utilization of actual work data: Delete completely after moving only minimum data and finishing work
For laptop computers, it is necessary to review measures to block arbitrary bring-out (anti-theft lock device, etc.)

2. Whether the disk is completely erased upon bring-out

For normal PC/laptop computer, it can be completely erased on the 2nd floor of the main door when bringing out, it is necessary to prepare a measure to erase computer equipment of unusual form by the field team (or discard the disk)

3. In case of not performing complete deletion: Self-review is required after checking the security review items when preparing the bring-out certificat

<Bring-out procedure for laptop computer/computer equipment by partner companies>

1. If data should be erased completely (utilization of actual data, etc.): Erase provided data and generated results completely

※ Deletion support: Office on the 2nd floor at the front gate (031-5172-2458) - Pre-scheduling is necessary.

2. Fill out the bring-out certificate, have it checked at the front gate and bring out.

Q3. What is the procedure for bringing out computer equipment when transferring from/to another area/headquarters?

[Manual] Information on the procedure for bringing out computer equipment due to personnel appointments (relocation, dispatch)

Overview: Information on documents required for bring out when moving computer equipment (PC, PWS) due to relocation (including dispatch)

Case1. Carry out complete deletion

- Required documents: Free bring-out certificate + official letter (arbitrary decision by the team manager) + Confirmation of complete deletion

- Confirmation of complete deletion is issued after complete deletion at the help desk (Namyang/Mabuk/Uiwang: District A 8080, others: 02-801-4321)

- For places of work that do not use the confirmation of complete deletion such as Luchen/Autoway Tower, it is replaced with the attachment of ITSM processing results (a separate request from the person in charge of deletion is required in case of complete deletion)

Case2. Complete deletion not carried out

- Required documents: Free bring-out certificate + official letter (arbitrary decision by the team manager)

Example of disposition form preparation

Title: Request for cooperation in bringing out computer equipment (PWS) due to team transfer

1. Reason: Bring out computer equipment (PWS) due to the relocation of place of work according to team transfer
2. Person: Researcher □ □ □ of OOO Team → User after change: □ □ □ (Company ID number: 1234567)
3. Place to move the equipment: OOO Team (Team code: OOOO-5, Namyang) → XXX Team (Team code: OOOO-1, Yangjae Headquarters)
4. Bring-out date: OOOO:XX:XX
5. Information on equipment to be brought out: (model name, control No., asset No., serial No.)
6. Complete deletion: Complete deletion carried out/not carried out

※ Attachment: Confirmation of complete deletion (issued by PC/PWS maintenance room) or a copy of trade secret bring out list

- Required

※ Cooperation office

- PC bring-out: R&D Information Protection Team, R&D General Affairs Operation Team, Team that the employee will be transferred to
- PWS bring-out: R&D Information Protection Team, PLM Promotion Team, Research Institute Technology System Team (HAE), Team that the employee will be transferred to
  R&D Finance Team, Regional Accounting Team (Accounting Team (Headquarters) or Ulsan Finance Team or Asan Finance Team or Commercial Business Management Team)

Precautions

- If the computer equipment is brought out, it must be moved to the team that the employee will be transferred to as soon as it is brought out on the same day.
  (ex. Bring out from the research institute when leaving work on Friday, bring it into the headquarters when going to work on Monday: not allowed)
- In principle, PCs should be returned to the regional General Affairs Team and a new one should be issued.

Employee ID reissuance procedure

How to apply for the reissuance of an employee ID card

STEP 1

Access Autoway Personnel System (HR-Lounge) Apply at > My Profile > Application Business > Apply for Employee ID Card

STEP 2

It is approved by the team manager and confirmed by the person in charge of employee ID card issuance

STEP 3

Collect it from the person in charge of issuance of the R&D Information Protection Team at the 2nd floor of the design 1 building.

※ Reference

- Until you receive your new employee ID card, use the temporary pass (collected at the information desk in each building).
- If the employee ID card is lost and reissued, a total of 5,700 won for the employee ID card (3500 KRW), case (600 KRW), reel holder (1600 KRW) will be deducted from the salary.
- In the case of reissuance due to reasons other than loss (malfunctioning, etc.), no separate deduction will be applied and the existing employee ID card must be returned.

How do I apply for an access pass for our affiliated company's employee who works at Namyang Research Institute?

You can apply by e-mail to the person in charge in the R&D Information Protection Team.

(Contents to be included in e-mail : Affiliated company's name / team name / employee's name / period of work / place of work)

FAQ

Q1. Is it possible to issue a long-term access pass for our affiliated company's employee who frequently accesses the research institute although he/she does not work in the research institute?

It is impossible. Please understand that issuance of a long-term access pass is very strictly managed for security purposes except for the staff members who work in the research institute to ensure the equality of all staff members including employees of our affiliated companies.

Access Pass Issuance Procedure for Partner Company's Employees

Information on the long-term access pass issuance procedure for employees of partner companies who work in the research institute is provided as follows. Please note that the issuance of a long-term access pass for people other than the following persons is not possible in accordance with the security policy and related laws.

Dispatched employees (includingperson in charge of general affairs and part-timers)	① Apply at Namyang Access Security System > Access Pass > Resident Companies > Employees ② Approve by the team manager of the field team ③ Confirm by the person in charge of access pass and send e-mail regarding information on pass collection.
Partner Company's employees working in the research institute	① Apply for issuance of the access pass for field manager (Apply for an access pass on the Employee ID Card Management System) ② Review the possibility of issuance by the R&D Information Protection Team ③ The partner company's employee comes into contact with HDS and applies for issuance of an access pass (HDS contact information : 02-2055-7993 / jhlee@hds-secu.com) ④ Apply for the field manager access pass (Send e-mail to the person in charge of R&D Information Protection Team) ⑤ After receiving the e-mail regarding the information on the collection of the pass for the field manager, visit and collect the access pass.
GE (Guest Engineer)	GE-related tasks are carried out by the field manager on the GE Operation System. (GE Operation System : AutoONE > Workspace > Support > GE Operation) **New** ① Apply on the GE Operation System through the GE application procedure. ② When the GE application is approved, the access pass will be applied automatically. ③ Confirm by the person in charge of access pass and send e-mail regarding information on pass collection. ④ After receiving the e-mail, bring the necessary documents to receive the access pass. ※ Necessary documents: Security pledge, Health Insurance Qualification Certificate (issued at the website of the National Health Insurance Corporation) **Reissuance** ① Apply for re-issuance at GE Operation System ▶ Access Pass ② Approve by the team manager of the field team/GE Operation Team ③ Confirm by the person in charge of access pass and send e-mail regarding information on pass collection. ④ After receiving the e-mail, bring the necessary documents to receive the access pass. ※ Necessary documents : Statement of reasons for re-issuance **Extension of period** ① Apply for period extension at GE Operation System ▶ Access Pass ② Approve by the team manager of the field team/GE Operation Team ③ Period extension of access pass is carried out by the R&D Information Security Team ※ Necessary documents: Submit Security pledge and Health Insurance Qualification Certificate additionally **Person in charge of GE Operation System:** Researcher Han Duksook of R&D Company Technology Support Team **Person in charge of Namyang GE access pass issuance :** Manager Pyo Soojin of the R&D Personnel Operation Team **Person in charge of Uiwang GE access pass issuance :** Manager Lee Seongwoo of the Design Support Team

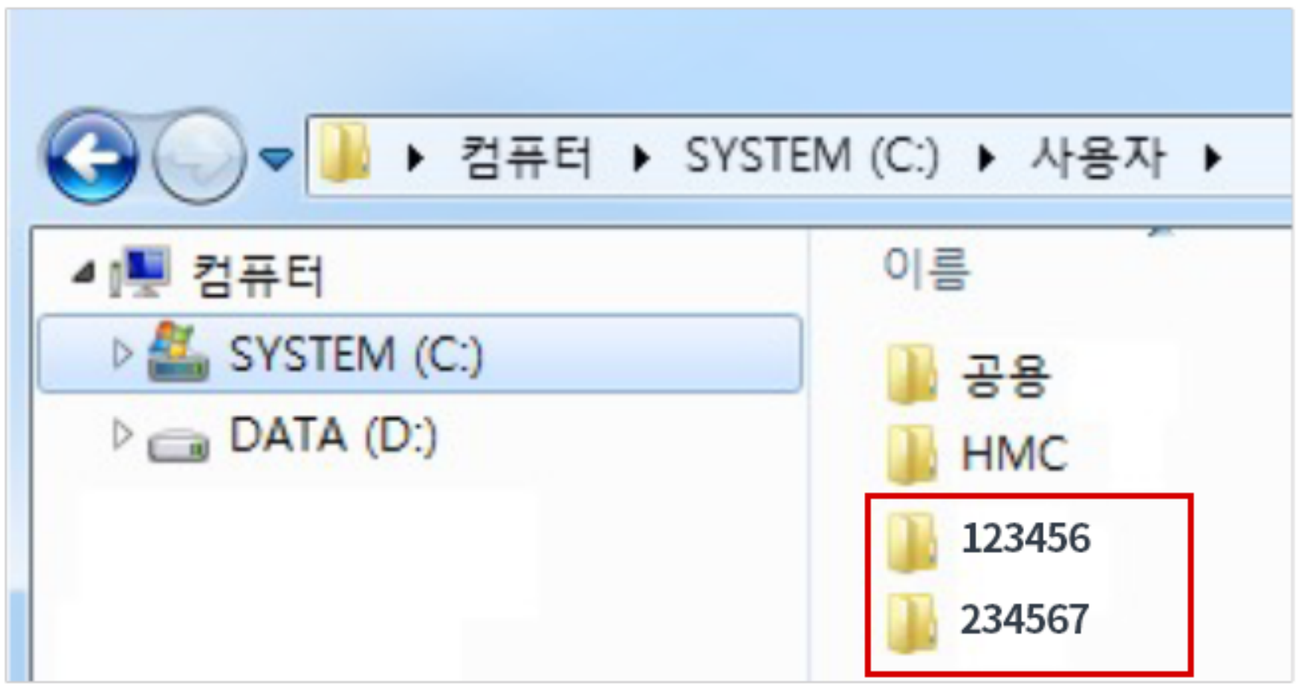
2 | Technology (PC/Network)

Integrated PC Management System (AD)

This is a system applied to use a stable operating system (OS) through periodic Windows updates,
and, after AD installation, the employee ID number or a public account is used to log in as a Windows user.

Q1. When installing/reinstalling AD, will the existing data be deleted?

Since AD is the task to set the Windows user environment, existing data will not be deleted when installing/reinstalling AD
However, after AD installation, user environment reset may change the path to the desktop folder.



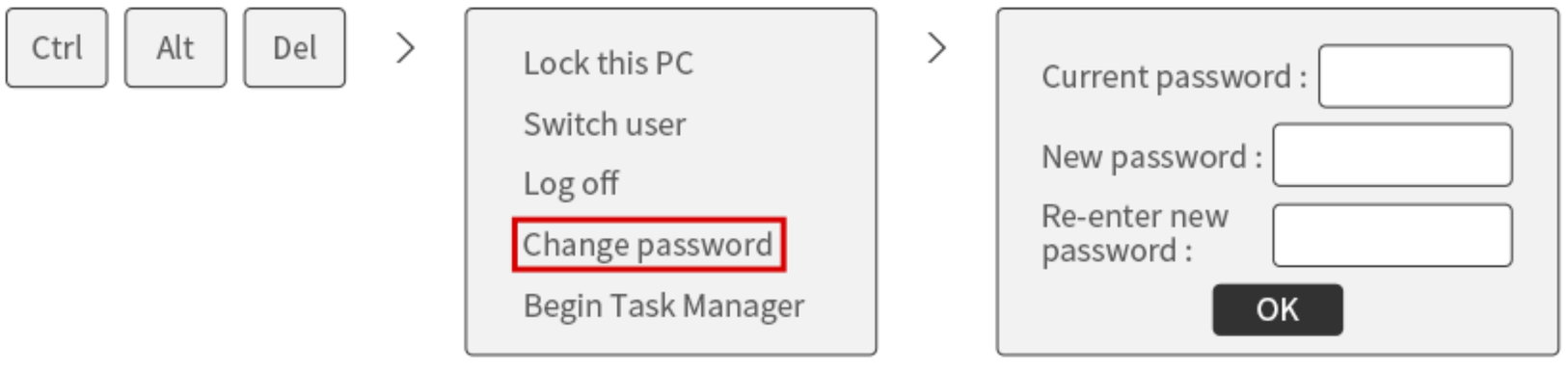
When installing/reinstalling AD, a user folder is created under the C:\Users folder for each user ID entered,
and folders such as the desktop are configured under that folder.

Q2. How can I change my AD password? (Including password reset)

When you change the Autoway password, the AD password is also changed in the same way.
However, it does not apply to team public accounts, etc., and it only applies to accounts with a 'company ID number'.
Team public accounts, etc. can be reset in the following way.

1) If you know the old password

① While logging in with the old password, press the 'Ctrl + Alt + Del' keys on the keyboard at the same time, and
② change the password from 'Change Password' menu.



2) If you do not know the old password

① Write the account name (team code, etc.) and send an e-mail to the manager (AD manager of the R&D Information Protection Team)

Q3. It says that the old team code account has expired. What should I do?

If the team name (team code) is changed due to organizational change, etc., the existing team account will be deactivated. Therefore, in this case, it is necessary to send an email with the correct old team name and team code to the AD manager of the R&D Information Protection Team. After receiving the email, the AD manager will guide you through the process to temporarily activate the account and change it to a new team account.

① Create a new folder under the C drive and copy and paste all the files on the existing desktop to the folder
(When switching accounts, desktop data is not deleted but is initialized)

② Access to http://www,hkmg.global and click the OK button at the bottom of the screen.

③ Enter a new account and password in the user ID input window (initial password)

④ When selecting New/Used during the process, select 'New'.

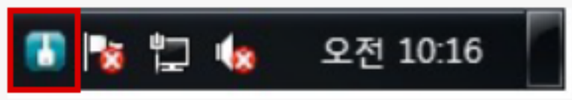
⑤ User will be changed through the rebooting process two times.

Information on DRM use

We introduced 「Document Security System, DRM (Document Rights Management)」 to encrypt important documents and manage permissions, and the system provides additional functions such as watermarking application when printing documents and the transmission of encrypted documents to the outside.

Document Security System (DRM) Login Window

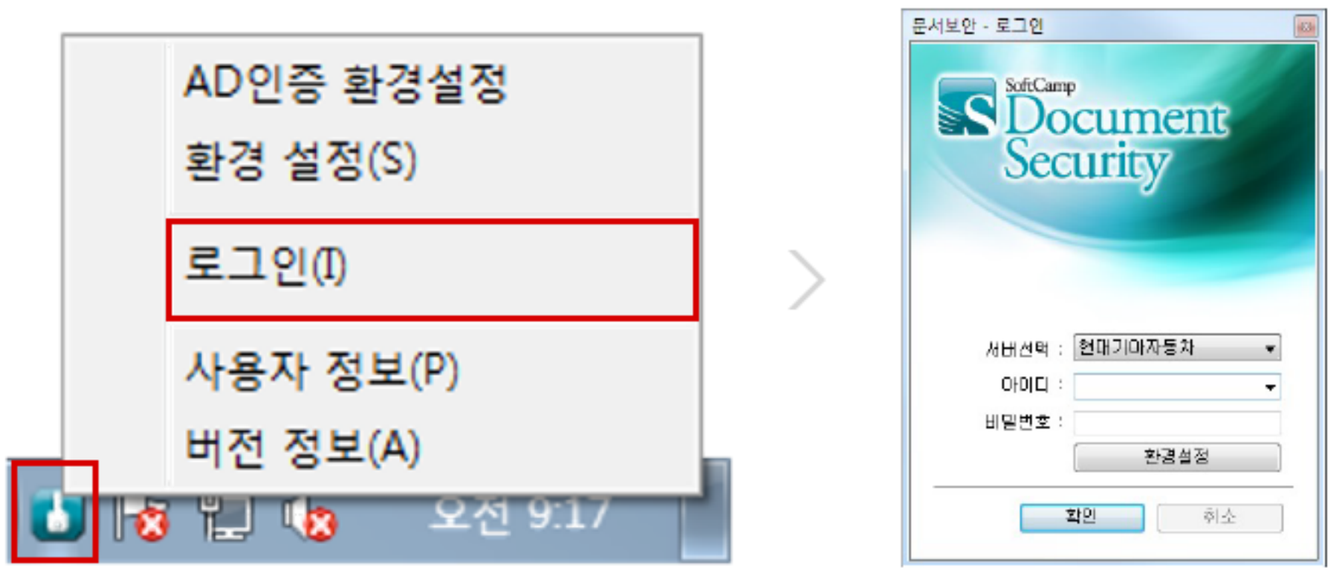
icon of a file encrypted by DRM



Icon of Document Security System (DRM) installed on PC

Q1. How to log into document security (DRM) again

If you need to re-login for document security, such as when using a public PC, please log in again by referring to the following.



① DRM icon on the taskbar

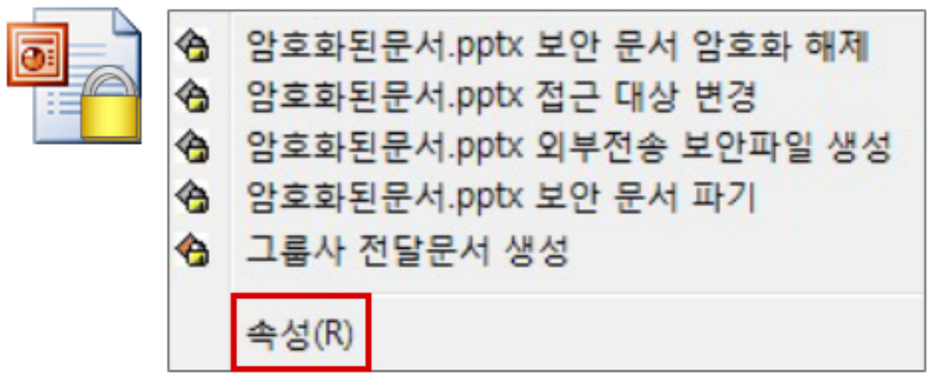
② Click the 'Login' menu and log in again.

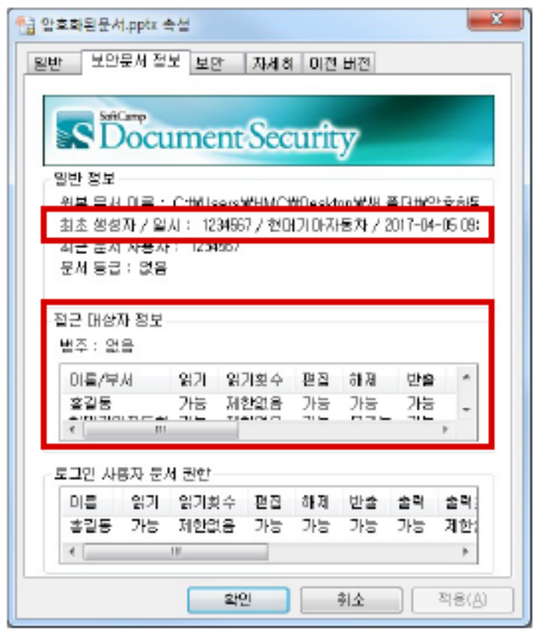
Q2. How to check the permission of an encrypted document

If you need to check whether the encrypted document can be decrypted, edited, or printed, please refer to the following.

① Right-click on the encrypted file and click the 'Properties' menu.

② Click the 'Security Document' tab and check the permission.





ID of the user
who encrypted this file
initially

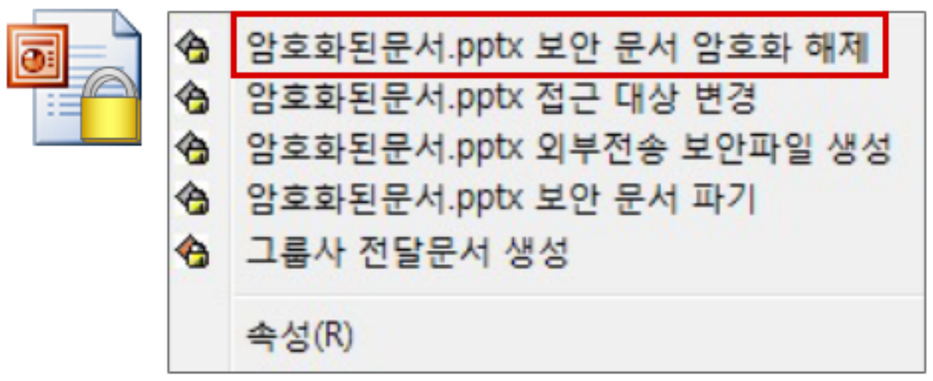
User(s) and permission
that can assess
this file

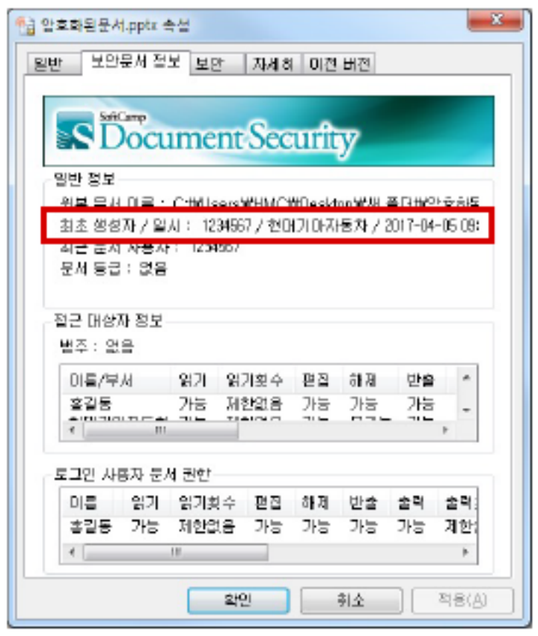
Q3. How to decrypt an encrypted document

If you need to decrypt an encrypted document, please refer to the following.

① Right-click on the encrypted file and click the 'Decrypt an encrypted document' menu.

※ You can decrypt it only if the original creator shown is your company ID number while you are holding the permission to decrypt by yourself. If you do not have the permission to decrypt of yourself or if the original creator is not you, you can decrypt it through the 'Security Document Decryption/Conversion Center' after obtaining approval from the department head. (How to access: Autoway > My Work > Secure Document Decryption/Conversion Center)



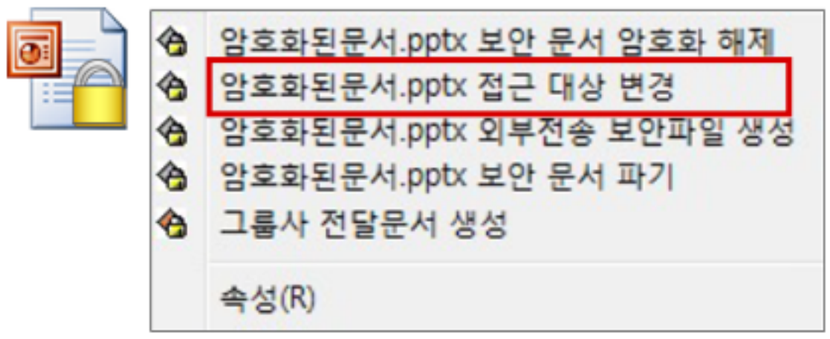


Q4. How to change the permission of an encrypted document

If you need to change permissions, such as expansion/reduction of persons who can gain access to the encrypted documents, please refer to the following.

① Right-click on the encrypted file and click the 'Change Access Target' menu.

② Add/modify/delete an access target



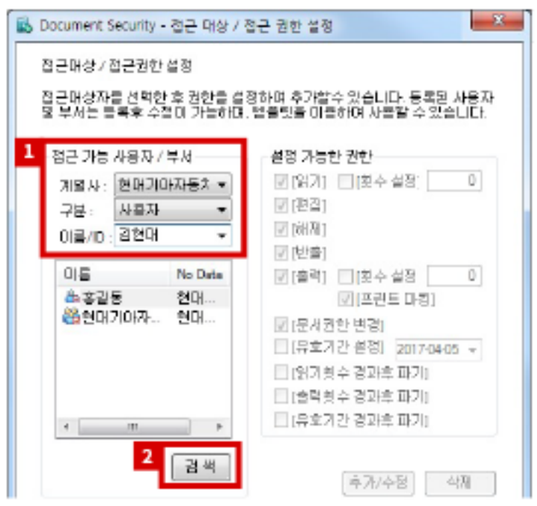
< Adding/modifying a permission holder >

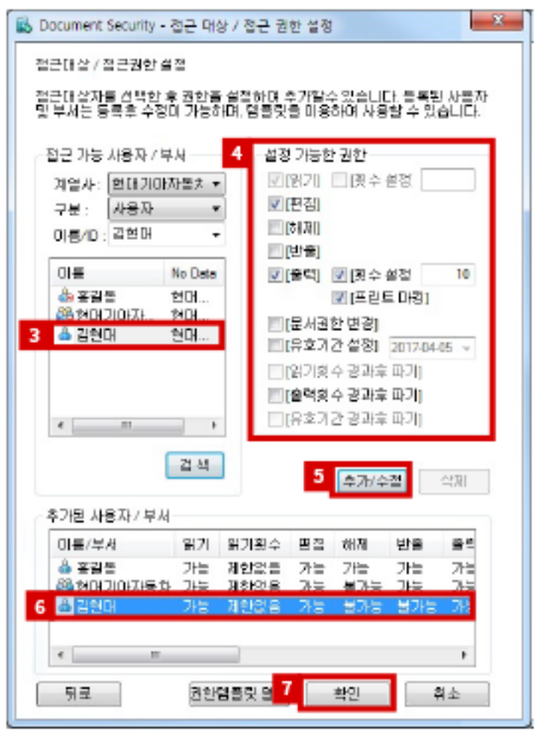
① Enter the user/organization name to be added in the Name/ID field. → ② Click the Search button.

③ Select the target to add/modify. → ④ Set permissions. → ⑤ Click the Add/Delete button. → ⑥ Check added/modified contents.

⑦ Click the OK button.

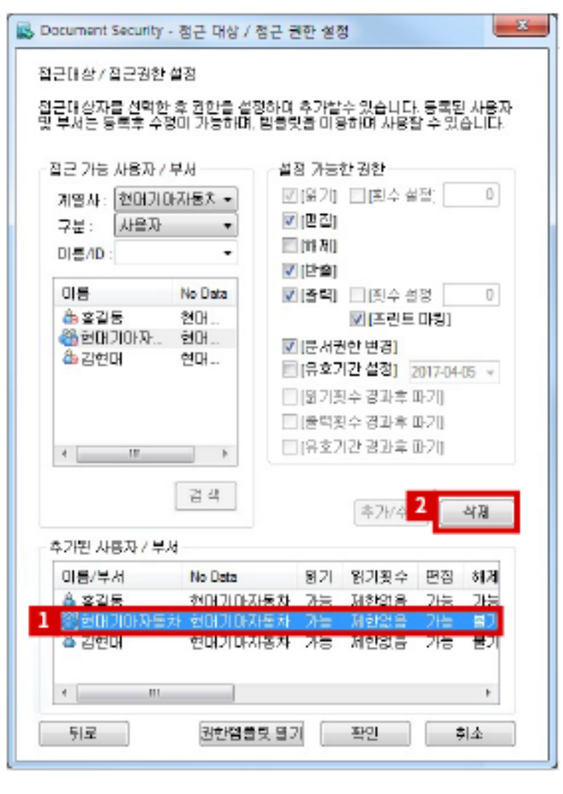
※ In the case of granting permission by team code, Reading/Editing will be impossible if the team name is changed.

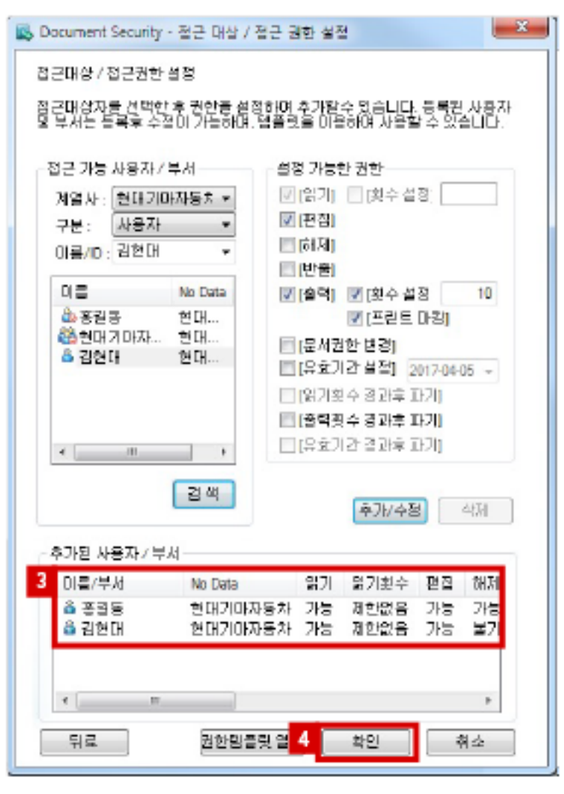




< Deleting a permission holder >

① Select the target to delete. → ② Click the Delete button. → ③ Check that the target has been deleted. → ④ Click the OK button.



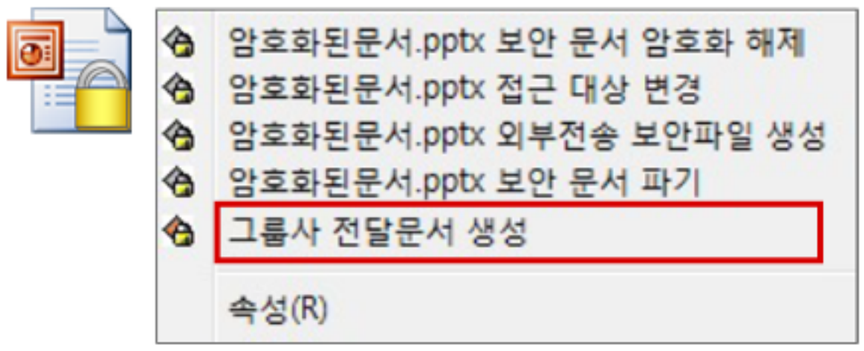


Q5. Creating a document to be delivered to the group company.

Encrypted documents can be delivered without decryption to affiliated companies that use the same document security system as Hyundai/Kia Motors. However, it is necessary to set the permission for the organization or user of the affiliated company that receives the document, and for how to set the permission, please refer to the following.

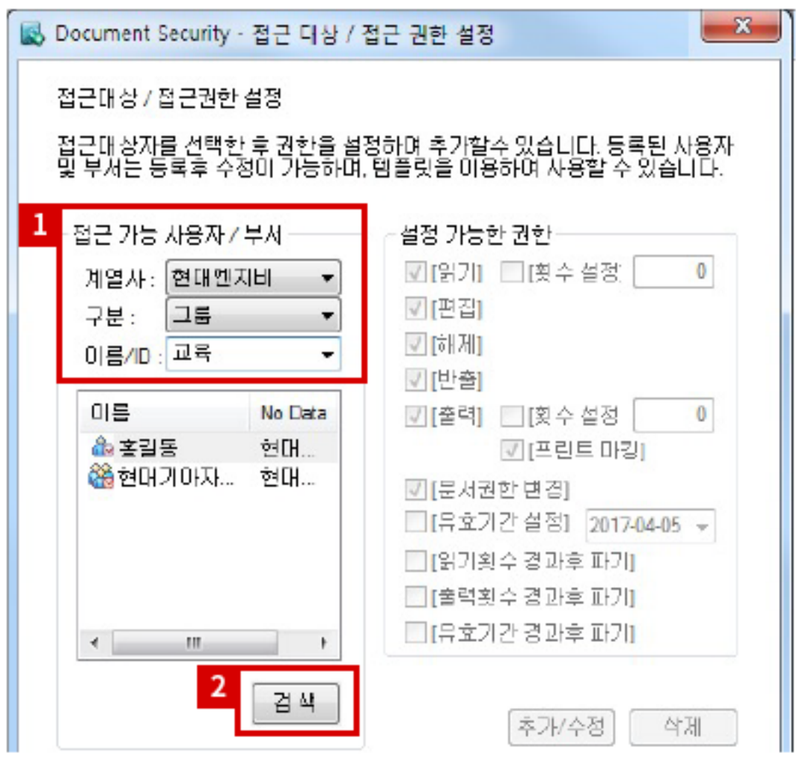
① Right-click on the encrypted file and click the 'Create a document to be delivered to the group company' menu.

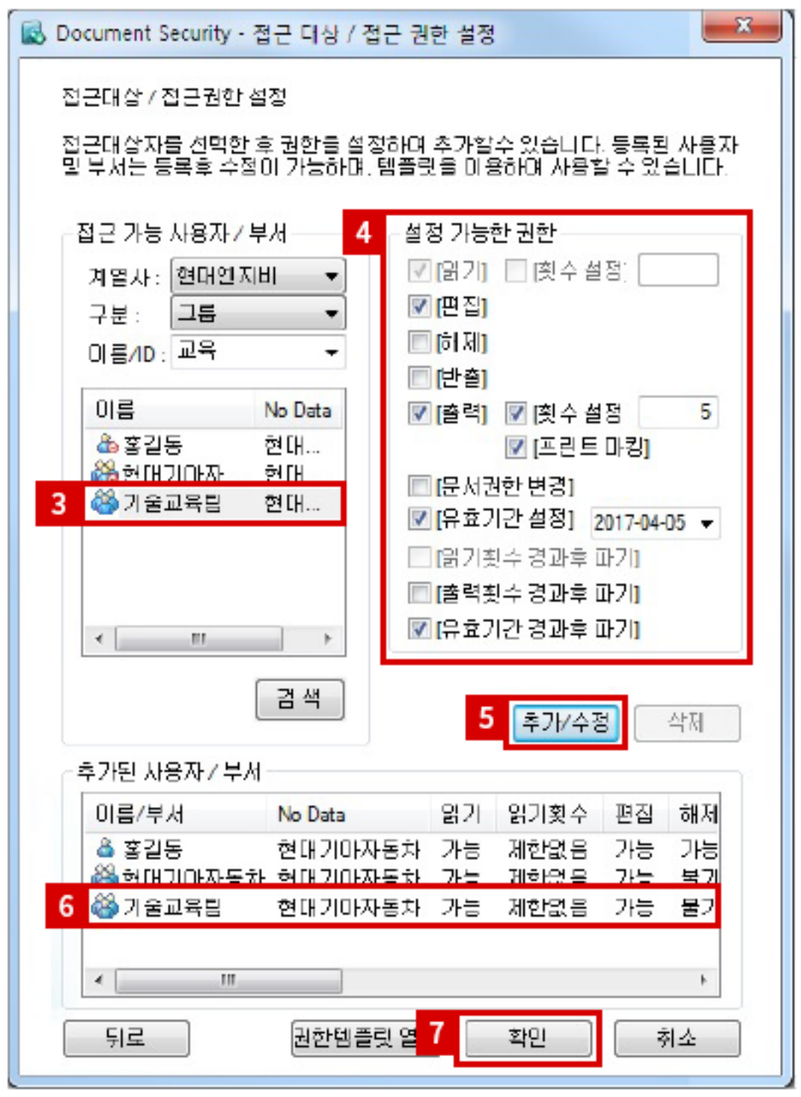
② After selecting the organization/user of the group company to which the encrypted document will be delivered, proceed with permission setting.



① Enter affiliated company, user/organization name. → ② Click the Search button. → ③ Select the target to add/modify.
④ Set permissions. → ⑤ Click the Add/Delete button. → ⑥ Check added/modified contents. → ⑦ Click the OK button.

※ In case of granting permission by team code, Reading/Editing will be impossible if the team name is changed.



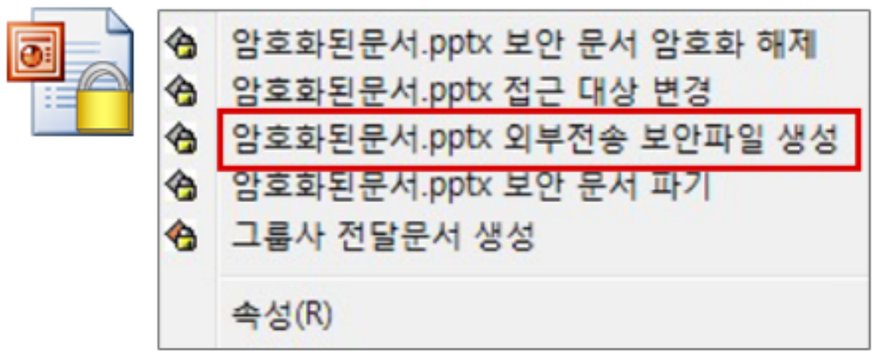


Q6. Creating a security file to be sent to the outside

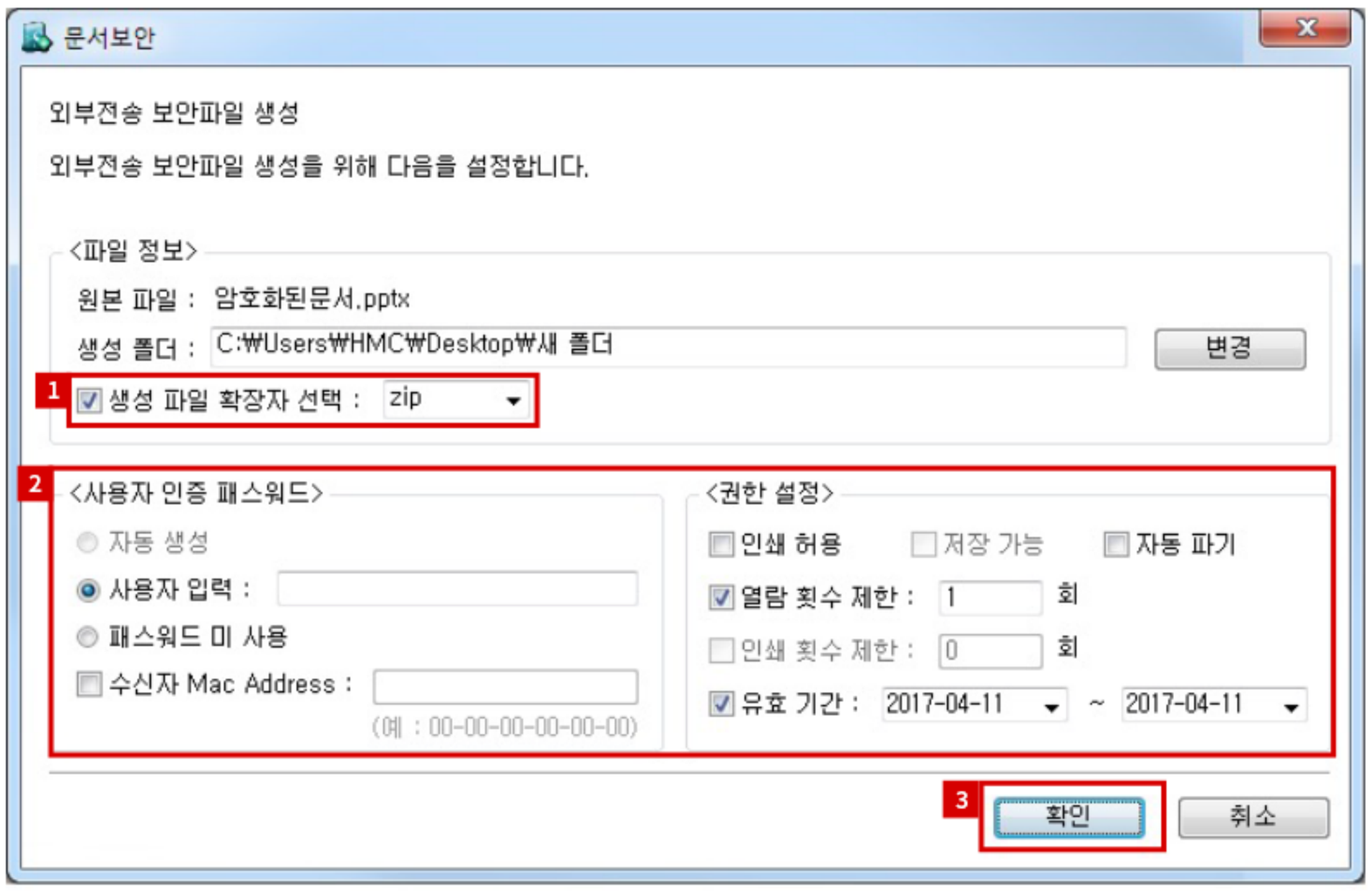
If you need to deliver encrypted documents to an external organization or a contractor that does not use our document security system, you can deliver encrypted documents without decrypting through the 'Create a security file to be sent to the outside' function. However, additional settings through the 'Create a security file to be sent to the outside' menu are necessary, and for such settings, please refer to the following.

① Right-click on the encrypted file and click the 'Create a security file to be sent to the outside' menu.

② Proceed with security setting



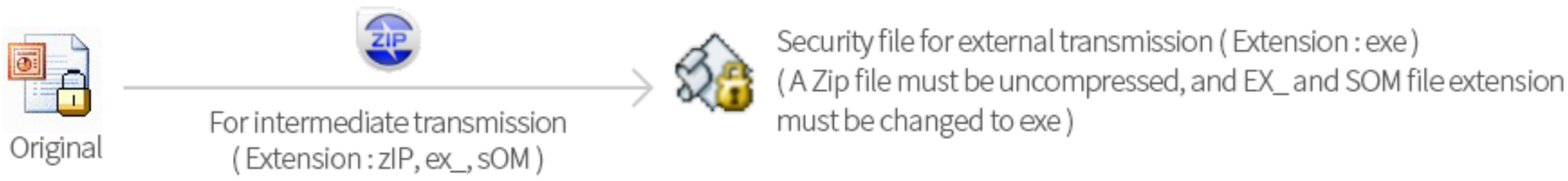
① Select the extension of the security files for external transmission. → ② Apply settings such as password, print, and expiration date. → ③ Click the OK button.



※ Refer to the following information when selecting the extension.

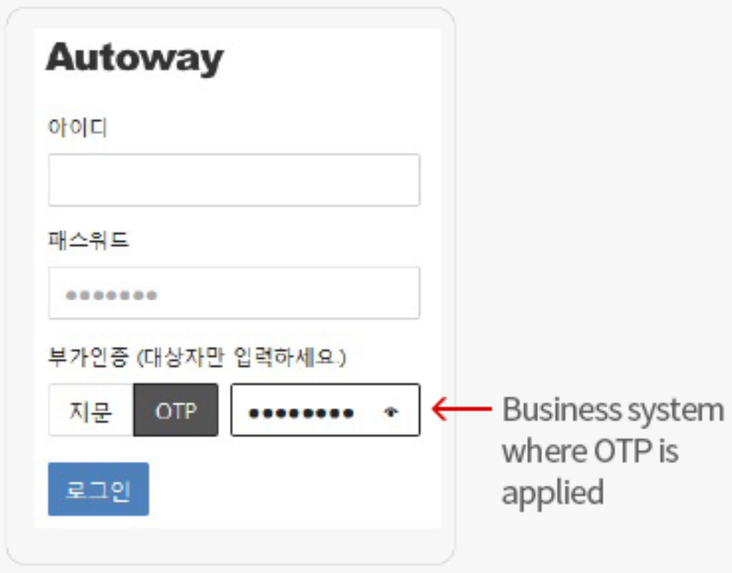
The extension of the security files for external transmission is exe. However, if the exe file is sent by e-mail, such e-mail may be misunderstood as a malicious code by the recipient and e-mail may be blocked.

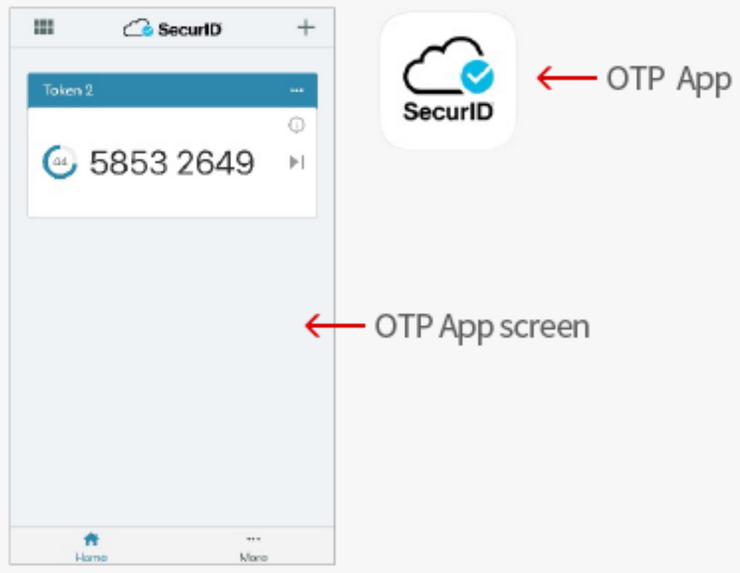
When creating a security file for external transmission, the system provides a function to create it in another format such as zip.



Information on OTP use

- OTP (One Time Password) is 「an additional authentication system」 applied to prevent account theft due to ID/PW leakage.
- When accessing business systems such as Autoway, you must enter an OTP code that changes every minute along with ID/PW.
  The OTP currently used by our company is based on the form of App installed on the smartphone.





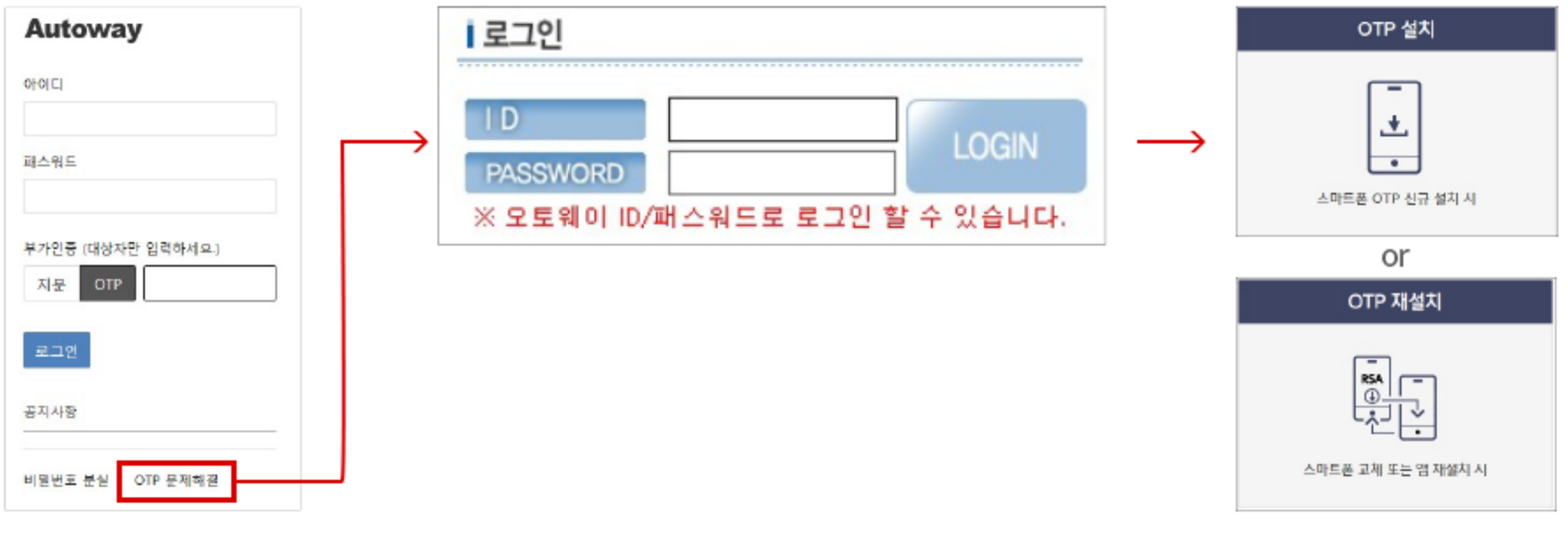
FAQ

Q1. How to install/reinstall OTP (changing smartphone, etc.)

① Access the App Store or Play Store on your smartphone and install the 'RSA SecurID' application.

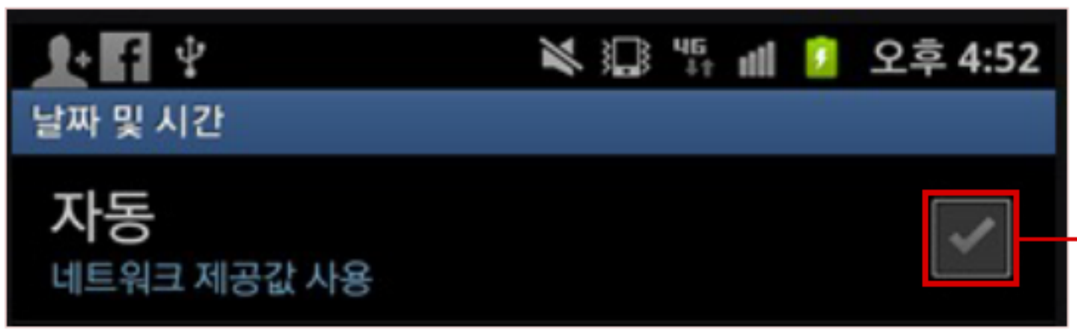
② Click the Solve OTP problem button at the bottom of the Autoway login screen on your PC.

After logging into the OTP management site, click the Reinstall OTP menu (in case of a new installation, the 'Install OTP' menu will be displayed)



Q2. When I log in, a message saying ‘The OTP number is invalid’ appears (the OTP is locked).

For normal use of OTP, the time on the smartphone must be set to ‘Use the value provided by the network’.
If a message saying 'The OTP number is invalid' appears even if this value is 'Use', reset the OTP time in the following way.



→ "Use" must be selected.

① Click the Solve OTP problem button at the bottom of the Autoway login screen on your PC (Refer to Q1).

After logging into the OTP management site, click the Reinstall OTP menu.

② Enter the token number displayed on the OTP twice and click the Reset Time button.

※ You must enter the current OTP token number and the next OTP token number that will change after 1 minute, respectively.

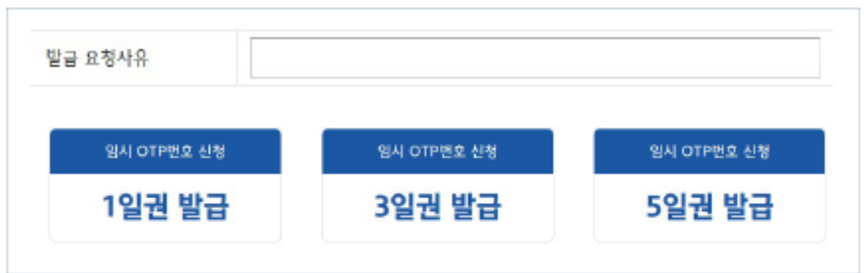
Q3. Is it possible to issue an temporary OTP number? (Smartphone lost, broken, not in possession, etc.)

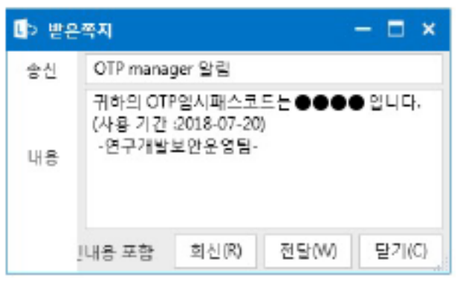
① Click the Solve OTP problem button at the bottom of the Autoway login screen on your PC. (Refer to Q1)

After logging into the OTP management site, click the Apply for a temporary OTP number menu.

② ‘ Enter 'Reason for Request for Issuance’ and , click the Apply for temporary OTP number button (Select among 1-day pass / 3-day pass / 5-day pass)

③ Check the temporary OTP number sent by mail, text message, or M-channel message.





※ Temporary OTP number will be sent by mail, text message, and M-channel message.

Information on use of removable storage device and secure USB

- Our security policy for removable storage devices such as normal USB and SD cards is 「Allow Reading, Block Saving」.
- When you need to save important documents to a removable storage device such as USB,
  we provide 'secure USB' that enables safe data management in preparation of security incidents such as theft/loss.

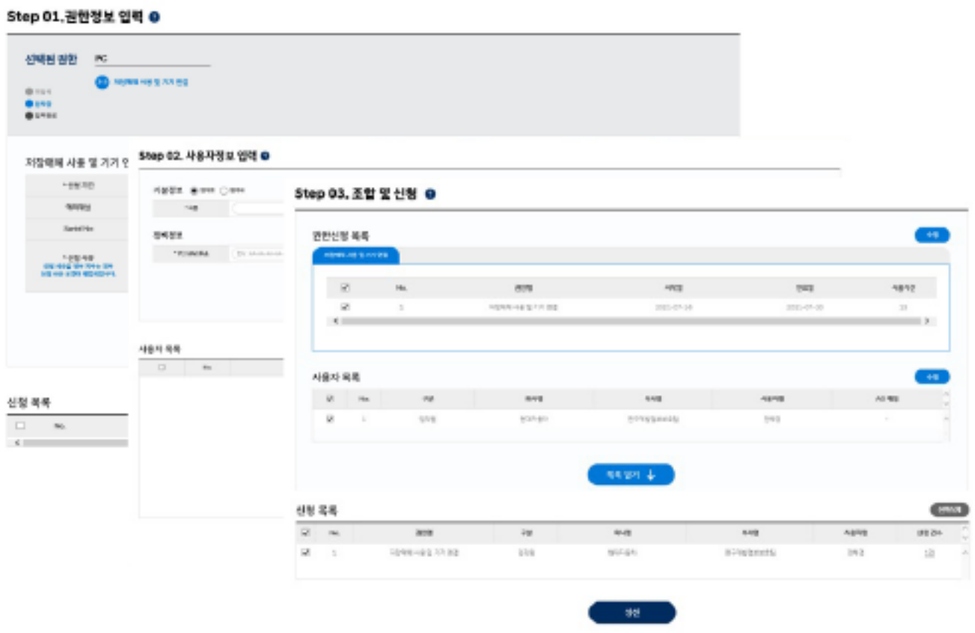
Secure USB

FAQ

Q1. How to apply for the permission to save on storage media such as normal USB

If you need to save a file in PC to a normal USB, please refer to the information below and proceed with the permission application procedure.

① Access Autoway > My Work > Access Security Permission Application System (SRMS)
- '2-3 Use Storage Media and Connect Device' > Click Apply for Permission
② Enter permission information and user information and submit for approval.



1. Enter permission information (Application period, exceptions, etc.) > Add to the list > Click 'Next'
2. Enter user information (user and equipment information) > Add to the list > Click 'Next'
3. Select the items prepared in ① and ② above > Add to the list > Select the application list > Click 'Submit'.

Q2. How to apply for a secure USB due to an additional new OR

In case a new or an additional secure USB is necessary due to the establishment of a new team or a part addition, etc.

① make a request to the person in change in the R&D Information Protection Team by e-mail.
(It is required to add the team leader of the team that applies for secure USB to the cc (carbon copy) list.)

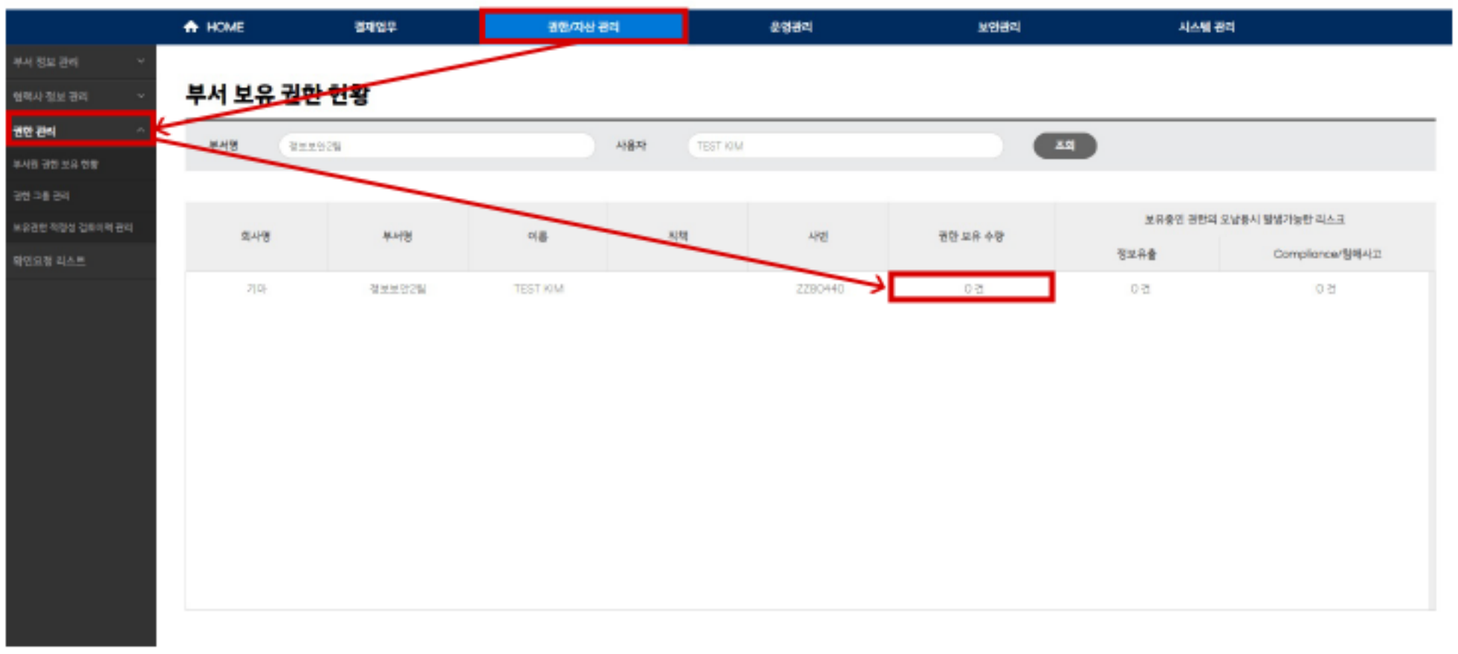
Applicant : Team security manager
Application detail
- Reason for application and quantity - Status of secure USB held in the team (※ only for an additional application)

Q3. Please let us know the status of the team members who have the permission on storage media.

If you need to check the information of team members who have the permission to save on storage media such as secure USB, please refer to the following.

① Autoway > My Work > Access to Security Permission Application System (SRMS) >
Select Permission/Asset Management > Permission Management > Select 'Status of Team Members Holding Permission'

② Inquire by the department name and check the quantity of permissions held by team members



Q4. Where can I check the status of secure USB holdings?

You can check the status of security USB holding as follows.

① You can check it from Autoway > Access to Security Portal > Asset Management > Status of Mobile Storage Media
(※ It can be checked only by the team security manager.)

Q5. Testing equipment says that secure USB is a prohibited equipment for use.

This is a message displayed by equipment that does not use the network if the secure USB has not been used for a long time.
Please take the following actions.

① Install secure USB on PC with internet connection > Log in > Re-install it to testing equipment and use.

VPN&VDESK

We provide VPN and VDESK systems to enable access to business systems from outside the company in the same environment as in-house when working from home or on a business trip.

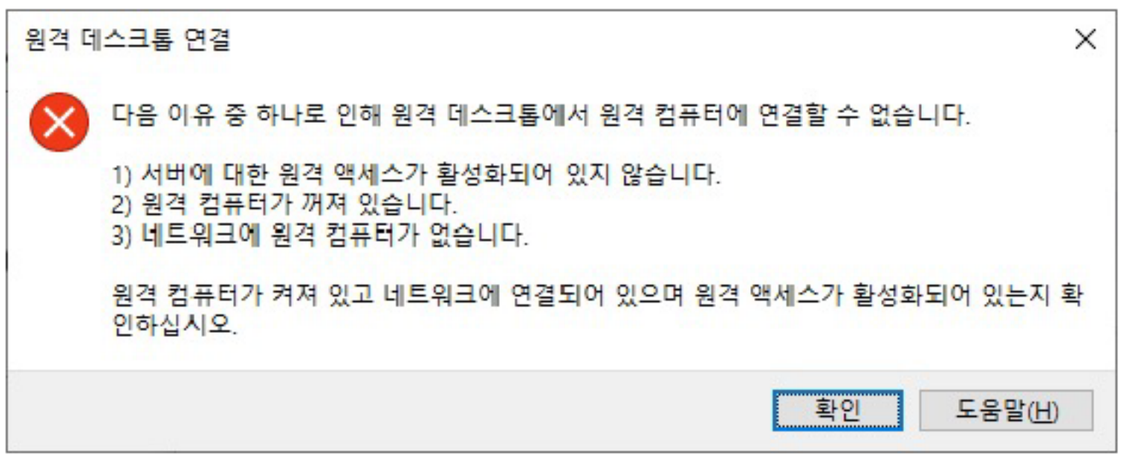
- A VPN (Virtual Private Network) can be used when using a company device, and an application for permission must be made in advance.
(Due to the current pandemic situation, all executives and staff members can use it, but only those with permission can use it after the situation ends)
- VDESK (Virtual Desktop) is a system that enables Autoway and document work in the virtual PC space when using a personal device.

FAQ

Q1. Remote access is blocked.

If remote access is not available, please check the following.

① If the following message is displayed

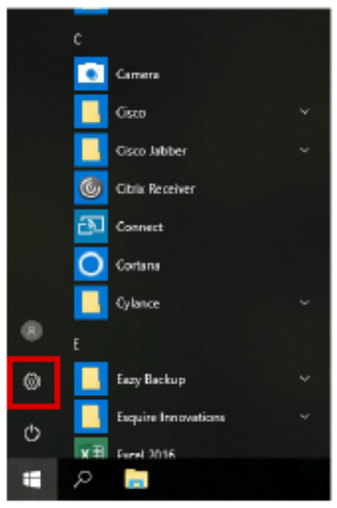


I) Check whether the in-house PC is booted and Internet use such as AUTOWAY is enabled.

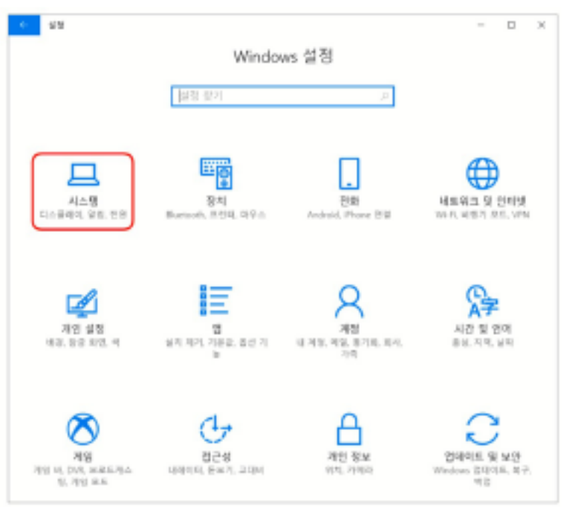
II) Check the VPN access URL: The VPN provided by Hyundai Motor Company is divided into headquarters/research institute, and you must access using the research institute VPN for remote access. (https://hkmc-rndvpn.Hyundai.net)

III) Check if the in-house PC environment is set for remote access (3 items).

1. Activating remote access



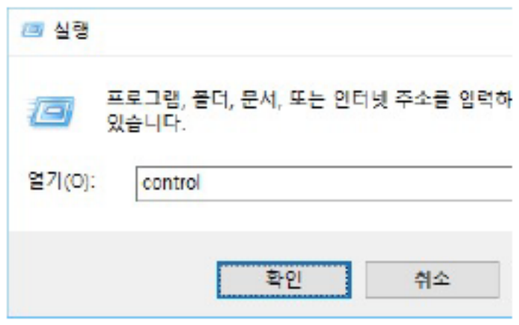
Click ‘Settings’ in the Start menu.



Click ‘System’

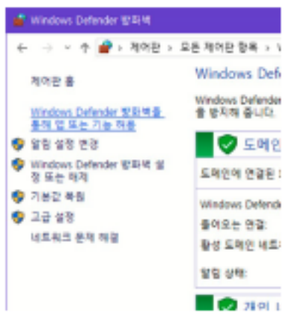
Set 'ON' for 'Remote Desktop Activation' item.

2. Setting Windows Firewall

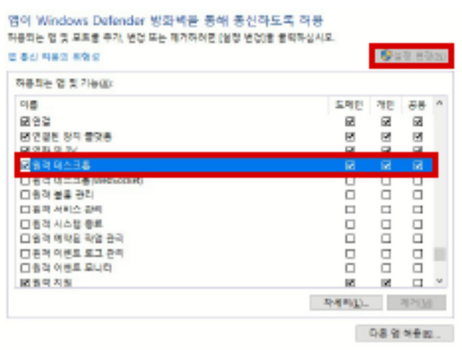


Press the
「Windows ( ) + R command
key to open the [Run] window.
→ Enter control to open the Control Panel.

Control Panel →
Click
Windows Defender Firewall.

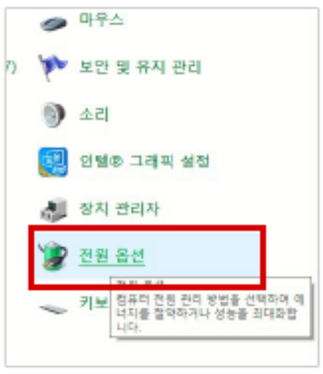


Click
‘Through Windows
Defender Firewall…’
on the left.



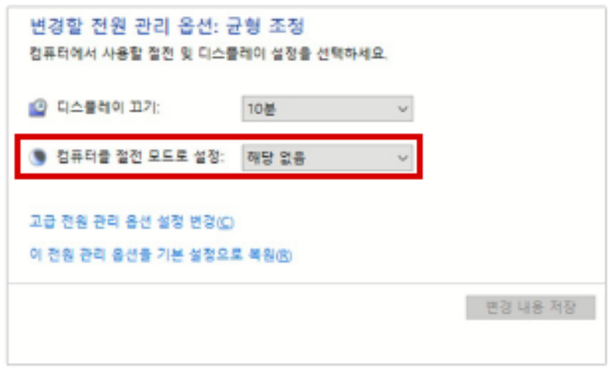
Put check mark on all
‘Remote Desktop‘ items
and press 'OK'.
※ If it is not possible,
click the ‘Change Settings’ button.

3. Canceling Power Saving Mode



Control Panel
→ Click 'Power Option'.

Click ‘Change settings’ of the currently selected item among items such as balanced adjustment, power saving, and high performance.



Change power saving mode to N/A and save.

② If the following message is displayed

I) Check user name: Need to check if it is entered as HKMC\Company ID Number.
II) Make sure that \ located above the Enter key on the keyboard is entered for the special symbol (\) after HKMC.

Q2. How can I gain access to VDESK??

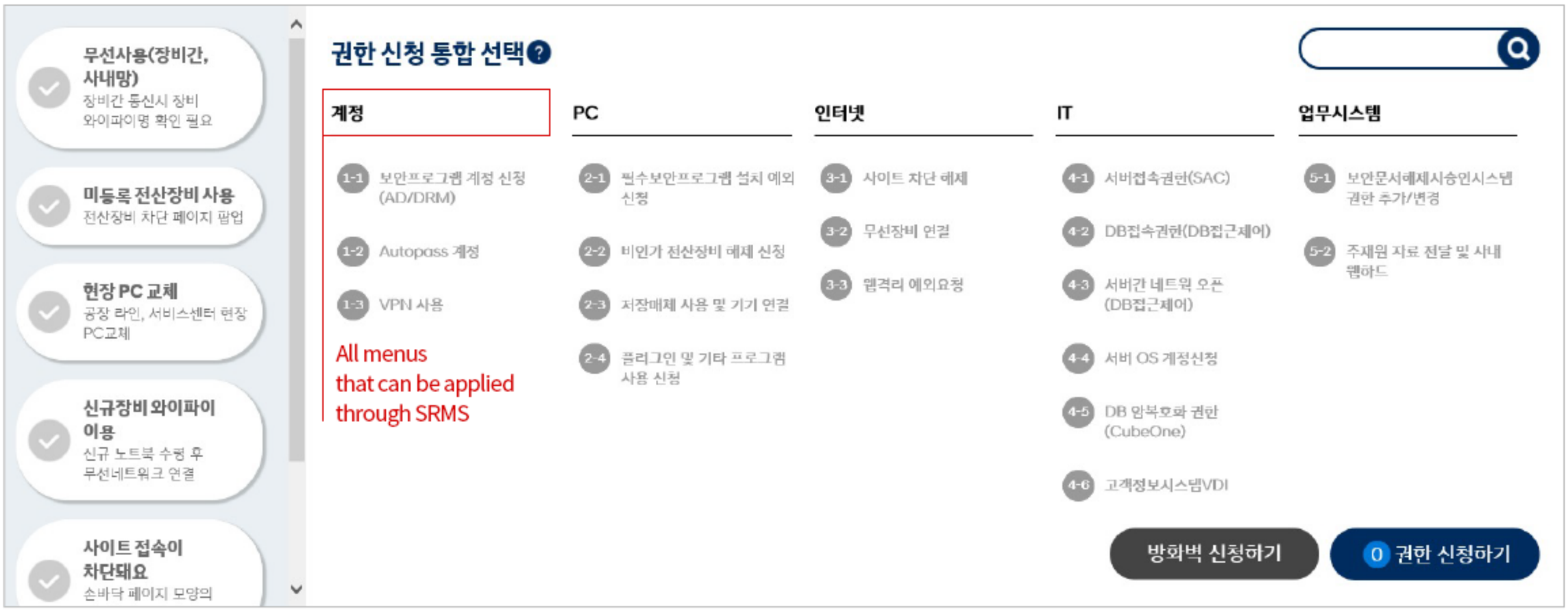
① Log into VPN	② Log into VDesk	③ Run virtual PC
https://hkmc-rndvpn.hyundai.net	https://vdesk.hmckmc.co.kr ※ Access after installing the required programs.	 Click the icon

Q3. I cannot see the file I saved from VDESK.

VDESK is a virtual space, and all the environments used when shutting down will be reset.
Make sure to send the file you created by e-mail before shutting down.

Access Security Permission Application System (SRMS)

The Access Security Permission Application System (SRMS) is a system designed to apply for security exception permissions necessary for business purposes and the system provides forms to fill out when applying for permission, so you can conveniently apply for permission.
(Autoway > My Work > Add My Work > Search for SRMS > Add to Favorites)



Network registration

Q1. I need Internet connection, but the message 'PC unregistered on the Network' appears on the screen.

Newly introduced equipment and equipment that has not been used for a long time are blocked from using the in-house network, so an application for network registration is required.
Application menu : [2-2] Registration of computer equipment on the network and security S/W exceptions

※ Prepare the following in advance.
① Applied period, reason for application
② User information, equipment information (IP address, MAC address, area to use PC, equipment classification)
③ Period of equipment use : Set for 5 years (in the case of partner company's equipment, it can be set up to 1 year, and if additional use is necessary, request for an extension)

Permission to save

Q1. I need to save the files on your PC/laptop to a USB device. (Normal USB device, SD card, etc.)

Since the storage of files to a mobile storage device is blocked by the security program, it is necessary to apply for the permission to use the mobile storage device.
Application menu : [2-3] Use of mobile storage device

※ Prepare the following in advance.
① Application period, exceptions, storage device information (Control No. or Serial NO, Device ID), Reason for application
② User information, equipment information (PC MAC address, Hostname)
※ Approval is given after registration of permission by our team, so the requested storage device can be used after approva

Q2. When I connect the equipment using a USB port, communication is not available.

If communication is not available when connecting to a PC/PWS/laptop computer using the USB port, please apply as follows.
① Access Autoway > My Work > Access Security Permission Application System (SRMS) - '2-3 Use Storage Media and Connect Device' > Click Apply for Permission
② Enter permission information and user information and submit for approval.

Wireless network

Q1. How do I apply for wireless use of the GDS diagnostic device?

GDS diagnostic device can only connect to the server wirelessly for diagnosis. (Internet use X, Work system use X)
Application menu : [3-2] Wireless device connection

※ When entering wireless router information, click the 'AP inquiry' button to search for RndMobile and select it (information will be entered automatically.)
※ Prepare the following in advance.
① User information: User's name, Team name, Position
② Equipment information: location (access point), IP address, MAC address
※ After approval process is completed, add a network in the Wi-Fi setting item of the tablet, set the network name as "RndMobile", set "CA certificate not authenticated", and enter Autoway ID/PW.

VPN

Q1. I'm on a business trip outside of the company, and I need access to the in-house system.

In order to access the business system in the same environment as in-house from the outside, it is necessary to apply for S/W VPN use.
Application menu : [1-3] VPN use

※ Prepare the following in advance.
① Purpose of application, period
② System information to access: system name, IP/Port, TCP/UDP
③ User information: User's name, Team name

Q2. I am on a business trip to an overseas research institute/factory, and I need to gain access to the domestic system.

If you cannot access the in-house system at the overseas research institute/factory, it is blocked by the overseas research institute firewall, and you need to check with the system manager and apply for the firewall to open.
Application menu : [Applying for Firewall] → Category of Application for Firewall : Select 'Open IDC Firewall'
If you unavoidably need to use the in-house system from the outside such as a hotel, etc. during a business trip, you need to apply for VPN use. (※ Refer to Q7)

※ Prepare the following in advance. (For applying for firewall)
① Purpose of application, period
② Server information at the point of departure/destination

Partner company AD/DRM

Q1. Partner company's employees must reside in the research institute for a certain period of time and use a PC, and document security and AD login ID are necessary.

In order to use a PC in the research institute, it is necessary to install the security program, and at this time, the partner company's employees must apply for ID separately. Application menu: [1-1] Apply for security program account (AD/ DRM)

※ Prepare the following in advance.
- Information of the partner company's employees: Company/Employee name, Existing ID (If exists)

Access to a blocked webpage from the inside of the company

Q1. There is a web page that I need to access for work, but it is blocked in the company.

Access to websites such as web hard, shopping, and stock sites is blocked within the premises, and if you need access for work purposes, you need to apply for access permission. Application menu : [3-1] Unblock a site

※ Prepare the following in advance.

① User information: User's name, Team name, Position

② Equipment information : IP address, MAC address

③ Blocked website address and access period

Q2. Partner company’s employees are using PCs in the in-house GE room and they say that there are sites and servers that cannot be accessed.

Since the in-house GE room is operated as a closed network, an application for communication permission is required to access the sites and servers required for work.

Application menu : Click the Apply for Firewall button -> Open OA Firewall (Partner company OA, VDI) -> Select OA Firewall GE network.

※ Prepare the following in advance.

① PC user information : Company name, user's name, department name, position

② PC location : Area (Namyang, Uiwang), Building name/Floor

③ PC information: MAC address, IP address

④ Information of sites/servers that require access: URL, IP/Port , TCP/UDP , host name, development/operation system, system administrator

⑤ Necessary access period

Application of permissions

Q1. After approval is given by the R&D information protection team, there is still a delay with the application.

For some requests for permission, it should be applied for through the system team. A request for permission is applied mostly on the day of approval, but in case a delay occurs, contact the following center.

Computer Help Center > Inside the company: Call (extension) 8080 and select 1, Outside the company: Call 02-801-4321 and Select 1

※ Prepare the following in advance.

① When requesting the Computer Help Center for delayed application of SRMS permission, deliver the approval number you applied for.

3 | Management (education/inspection)

Status of security-related business standards

The following is the status of security-related work standards registered in our company.
You can view the contents of work standards from Auto Way – My Work – Work Standards.

Name of Work Standard	Registration No.	Prepared by
Security Regulation	HR-BS-CM-007	Hyundai Information Protection Center
Security Management Regulation for National Core Technologies	HR-IS-BA-007	Hyundai Information Protection Center
Access Control for Namyang Research Institute.	HR-EB-CM-014	R&D Information Protection Team
Security Guidance for computer equipment Users	HR-BS-CM-058	Hyundai Information Protection Center
Security Management for computer equipment in the Research Institute	HK-EB-CM-001	R&D Information Protection Team
Information Assets Classification and Management Procedure	HR-IS-BA-004	Hyundai Information Protection Center
Security Management for Technical Data of the Research Institute	HR-EB-CM-075	R&D Information Protection Team
Security Accident Response and Management Procedure	HR-BS-CM-030	Hyundai Information Protection Center
Security Management Regulation for New Vehicles	HR-IS-BA-002	Hyundai Information Protection Center
Security Organization Composition and Management Procedure	HR-BS-CM-029	Hyundai Information Protection Center
Security Inspection and Audit Procedure	HR-BS-CM-031	Hyundai Information Protection Center
Security Authentication System for Technical Service Partners of R&D Headquarters	HR-EB-CM-016	R&D Information Protection Team
Mobile Security Guidance	HK-IT-JS-012	Hyundai Information Protection Center
Security Operation Manual for Information Technologies	HK-IT-JS-004	Hyundai Information Protection Center

Major security-related Acts

Status of Technology Leakage-related Laws

① Unfair Competition Prevention and Trade Secret Protection Act

: Prevent acts of unfair competition and infringement of trade secrets of others

Classification	Details	Penalties
Acts of release and infringement (Article 18)	- Acquisition, use, release, leakage, refusal of returning trade secrets - An act of acquiring or using trade secrets by theft, deception, coercion, or other improper means - Unauthorized release of trade secrets outside the designated place	Overseas: Imprisonment for not more than fifteen years or a fine not exceeding 1.5 billion won Domestic: Imprisonment for not more than ten years or a fine not exceeding 500 million won

※ The term "trade secret" means information, including a production method, sale method, useful technical or business information for business activities, which is not known publicly, is managed as a secret, and has independent economic value.

② Act on Prevention of Divulgence and Protection of Industrial Technology

: To prevent undue divulgence of, and protect, industrial technology in order to strengthen the competitiveness of Korean industries and contribute to national security and development of the national economy

※ Status of our industrial technologies designated as national core technologies

① Technology for the design and manufacturing of gasoline direct injection (GDI) type fuel injection systems

② Technology for the design and manufacturing of hybrid and electricity-based motor vehicle (xEV) systems (limited to control units, batter management systems, and regenerative braking systems)

③ Technology for designing, processing and manufacturing of fuel cell systems(hydrogen storage and supply systems, stack and BOP)

④ Technology for the design and manufacturing of LPG Direct Injection (LPDi) fuel injection system

⑤ Technology for the design and manufacturing of fuel injection systems, forced induction systems, and exhaust gas aftertreatment devices for diesel engines satisfying EURO6 emission standard or higher (limited to DPF and SCR)

⑥ Technology for the design and manufacturing of engines and automatic transmissions for motor vehicles (limited to technology developed not more than (2) years after mass production)

⑦ Technology for the design and manufacturing of core components and systems of autonomous vehicles (Limited to the camera system, radar system, rider system and precision locating system)

※ "National core technology" is a technology designated under Article 9 that may have a significant adverse impact on national security and national economic development if leaked overseas due to its high technical and economic value or high growth potential of related industries.

Classification	Details	Penalties
Acts of release and infringement (Article 14)	- Acquiring, using and disclosing trade secrets by theft, deception, coercion, or other improper means - Leakage, disclosure or provision to a third party by a person who is liable for the confidentiality - Acts of exporting, conducting cross-border acquisition, merger, etc. by improper means	Overseas - National core technology : Imprisonment for more than three years or a fine not exceeding 1.5 billion won - Industrial technology : Imprisonment for not more than fifteen years or a fine not exceeding 1.5 billion won Domestic : Imprisonment for not more than ten years or a fine not exceeding 1 billion won
Illegal use (Article 14, No. 4/No. 8)	Using illegally collected industrial technology without knowing, by gross negligence Using or disclosing industrial technologies for any purpose other than the purpose for which such information was provided	Imprisonment for not more than three years or a fine not exceeding 300 million won
Duty of Confidentiality (Article 34)	- Leaking or using any secret he or she has learned in the course of conducting his or her duties	Imprisonment for not more than five years, the suspension of qualification for not more than 10 years or by a fine not exceeding 50 million won
Measures for Protection (Article 10, Paragraph (3))	- Refuse or interfere with the measures for protecting national core technologies	An administrative fine not exceeding 10 million won
Report on Infringement (Article 15, Paragraph (1))	- No reporting in case the Infringement of a industrial technology developed as a national core technology or under the national R&D project or an accident occurs.	An administrative fine not exceeding 10 million wonzv

③ Criminal Act

Classification	Details	Penalties
Embezzlement (Article 355, Paragraph (1))	- A person who, having the custody of another's property, embezzles or refuses to return it	Imprisonment for not more than five years or a fine not exceeding 15 million won
Breach of trust (Article 355, Paragraph (2))	- A person who, administering another's business, obtains pecuniary advantage or causes a third person to do so from another in violation of ones duty, thereby causing loss to such person	Imprisonment for not more than five years or a fine not exceeding 15 million won
Occupational embezzlement, occupational breach of trust (Article 356)	- Occupational embezzlement or occupational breach of trust in violation of the duties of one's occupation	Imprisonment for not more than ten years or a fine not exceeding 30 million won

Daily security for the research institute

Thorough ID and PW management

Do not write ID and PW down on a post-it and attach it to PC or disclose them to others.

Prohibition of Leaving Documents Unattended on the Printer/Copy Machine

Do not leave business-related documents unattended on the printer, copy machine, scanner, etc.

Prohibition of Leaving Documents Unattended

Do not leave a document in places such as an empty seat, on top of a cabinet, in a conference room, etc. where it can be viewed by others.

Paper Shredding

A document which is no longer necessary or whose purpose of business has been accomplished should be shredded and discarded by means of a paper shredder.

Clean Desk

Always keep your desk neat and clean. Store documents, diaries, security USB, etc. used in a locked cabinet when leaving the office.

Wearing of an Employee ID Card

Always wear your employee ID card.

Visitor Management

All visitors should be accompanied by an employee at all times.

Prohibition of Disclosing/ Posting In-company Information to the Outside

Do not disclose or post company and business-related information to the outside.

Prohibition of Using Unauthorized Equipment

Do not use unauthorized computer equipment (including filming media). Use such equipment in accordance with the relevant procedure in case of necessity.

How to report on a security accident and handling procedure

Definition of a security accident

- A security accident is the disclosure, leakage, loss, and leakage of trade secrets due to an intentional act or negligence of internal/external personnel, the destruction of important facilities and equipment, illegal intrusion into protected areas, and any other activities that may cause disruption to management of the company by violating security regulations and various procedures.

Operation of information leakage reporting center

Targets for reporting	Center for reporting
- If the leakage of our trade secret or such fact has been confirmed - If the fact of an employee collecting a trade secret irrelevant to his/her business without permission has been confirmed - If the fact that a photo of our vehicle that is not released yet is posted on the Internet, etc. has been confirmed - If the fact that an unauthorized person entered our workplace and took an unauthorized picture has been confirmed	- Contact Information (031-368-1000, 6749 / R&D Information Protection Team) - It is operated for 24 hours a day, 365 days a year.

Security accident handling procedure

Divisions (including security team) recognize and respond to the fact	Response by the division handling security task

Recognize information leakage > Confirm the fact > Take initial responses > Report to the police and inform the company > Carry out detailed investigation and establish a measure to prevent the recurrence > Report on completion

※ Inform immediately after the recognition of the accident / Inform additionally after confirming the fact

Tip-off from the inside/outside of the company (intelligence)

- Phone (T 1000)
- Autoway mailbox

Internet searching

Request an outside agency

Security inspection / detection

Verify leaked information

- Importance of information
- Verify the range of information leakage
- Confirm/interview with the person who leaked the information

Center for reporting

R&D Information Protection Team
(031-368-1000 / 6749)

↓

Violation of the Act on Prevention of Divulgence and Protection of Industrial Technology

Linkage with an outside agency

- National intelligence service
- Korean National Police Agency Cyber Bureau, etc.

- Degree of danger for leaked information
- The measure to prevent its recurrence
- Disciplinary action (tentative) against the violator, etc.

↓

Alert the fact to relevant divisions

CISO : Hyundai Information Protection Center

Security planning team/Legal affairs/ Purchase

- Consult security divisions
- Announce the measure to prevent its recurrence
- Take disciplinary action against the violator
- Inform regarding the result of measure (to the whistleblower)

↓ Decision making by the management

Linkage with an outside agency

- Judicial action

FAQ

Q1. What should I do if a security accident occurs such as taking a picture without permission during a test conducted outside the company?

If a security accident occurs outside the company, inform the R&D information protection team of such fact and consult with the team.
Take necessary initial measures (covering with a camouflage cover, etc.)

Q2. What should I do if a laptop computer provided by the company gets lost or stolen during an overseas business trip?

If an accident such as loss or theft of a laptop computer occurs during an overseas business trip, report to the local police on such fact, receive the confirmation, and inform the R&D information protection team and the equipment management division of such fact.
In the future, report to the R&D information protection team and equipment management department with a confirmation of facts and a report of theft attached to the official document ※ In the case of an overseas business trip, be sure to bring only minimum data that fits the purpose of the business trip and carry out business using a laptop computer provided by the company.

How to classify and indicate document security levels

Classification of Security Documents (Document Security Level)

1) The classification of a security document is carried out by the initial information asset producer of the document.

2) The department (team) security manager has the permission to adjust the security level of the document and is responsible for managing and supervising the range of document distribution.

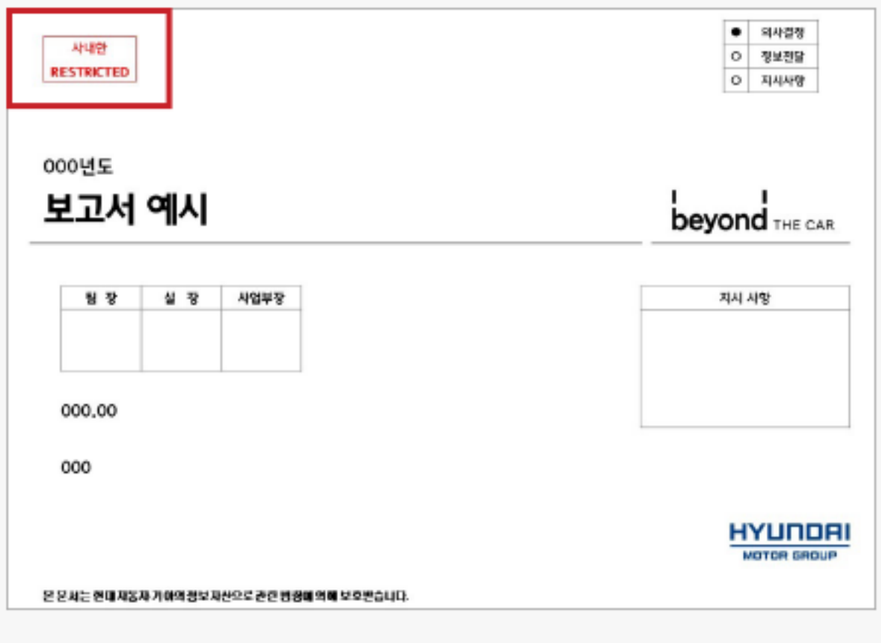
3) If the document includes contents of different security levels, a higher security level should be assigned.

4) The security level should be decided by considering the following classification criteria when the security document is classified, and the In-company restricted or higher level should be assigned to all created documents including documents in preparation for management.

Classification	Classification Criteria	Reference for Classification
Restricted	A document which may result in a loss to the company if it is leaked outside the company	If the importance of the document is lower than that of Top Secret/Secret-level documents produced by the company
Secret	A matter that may interfere with efficient execution of important company policies and result in financial loss	- If more limited access than a restricted-level document is necessary - If it is distributed to limited recipients - If arbitrary duplication and redistribution should be blocked
Top Secret	An item that may have a serious effect on the company management or will likely result in a great loss to the company if it is used by a competitor or a stakeholder	- If more limited access than a Secret-level document is necessary - If strict management is necessary when a printed document is distributed - If it is impossible to be distributed in form of electronic document - If a special physical protective measure is necessary for storing a printed document

Indication of Document Security Level

The corresponding security level should be indicated at the top left or top right side of all pages of the document.



Security pledge for executives and staff members

Pledge for trade secret protection

The pledge for trade secret protection is the basic pledge for security that all executives and staff members of Hyundai Kia Motors are required to prepare. Information on the period for each target and the method of preparation is provided below.

Classification		Period	Method of preparation
New/Experienced		Initially at the time of entrance	Pledges are collected and stored by the personnel team
Senior researchers / Senior Manager	Change of team/division (based on the team code)	Quarterly	① An e-mail is sent to all eligible recipients quarterly. ② After receiving the email, prepare the pledge through the URL and receive approval from the team manager. ③ Check the system (Pledge management system) and store the pledge.
	Promotion to senior researcher		
Executives			Pledges are collected and stored by the personnel team

Preparing the pledge for the national core technology protection

The pledge for the national core technology protection is the pledge required additionally from employees who handle national core technologies for business purpose in addition to the pledge for trade secret protection (according to Article 10 of the Act on Prevention of Divulgence and Protection of Industrial Technology)

What is a national core technology ?

※ It means an industrial technology designated by the government under Article 9, the unauthorized divulgence of which abroad could have a material adverse effect on national security and development of the national economy, since it has high technological and economic values in the Korean and overseas markets or brings high growth potential to its related industries.

List of designated national core technologies in automotive

① Technology for the design and manufacturing of gasoline direct injection (GDI) type fuel injection systems

② Technology for the design and manufacturing of hybrid and electricity-based motor vehicle (xEV) systems (limited to control units, batter management systems, and regenerative braking systems)

③ Technology for designing, processing and manufacturing of fuel cell systems(hydrogen storage and supply systems, stack and BOP)

④ Technology for the design and manufacturing of LPG Direct Injection (LPDi) fuel injection system

⑤ Technology for the design and manufacturing of fuel injection systems, forced induction systems, and exhaust gas aftertreatment devices for diesel engines satisfying EURO6 emission standard or higher (limited to DPF and SCR)

⑥ Technology for the design and manufacturing of engines and automatic transmissions for motor vehicles (limited to technology developed not more than (2) years after mass production)

⑦ Technology for the design and manufacturing of core components and systems of autonomous vehicles (Limited to the camera system, radar system, rider system and precision locating system

Preparation target

All executives and staff members who handle national core technologies in the automobile field for business purposes

Period and method of preparation per target

Classification	Method of preparation
All executives and staff members belonging to the relevant business division	Every 2 years (An official letter and e-mail are sent)
New employees/transferred employees	Pledges are collected and managed by the team security manager. (Refer to Security Portal – Security Manual – Prepare Pledge for National Core Technology Protection by New Employee/Transferred Employee)

FAQ

Q1. Where I can view the pledge of security that I prepared?

You can view it from ‘Pledge Inquire’ after accessing Autoway My Work ‘Pledge management system’.

Q2. Can I view the status of pledge preparation within our team (division)?

The team leader and the team security manager can view the pledge status of the team.
You can view it from "Pledge Inquiry" on the left after accessing to the pledge management system and checking if the team manager or the team security manager is selected from the combo box at the top right side.

Q3. I prepared the pledge incorrectly and I need to prepare it again.

If you need to prepare the pledge again, make a request to the person in change in the R&D Information Protection Team by e-mail. A reply will be sent to allow you to prepare the pledge again.

Q4. There is an employee in the team who is on a leave of absence. What can he/she do?

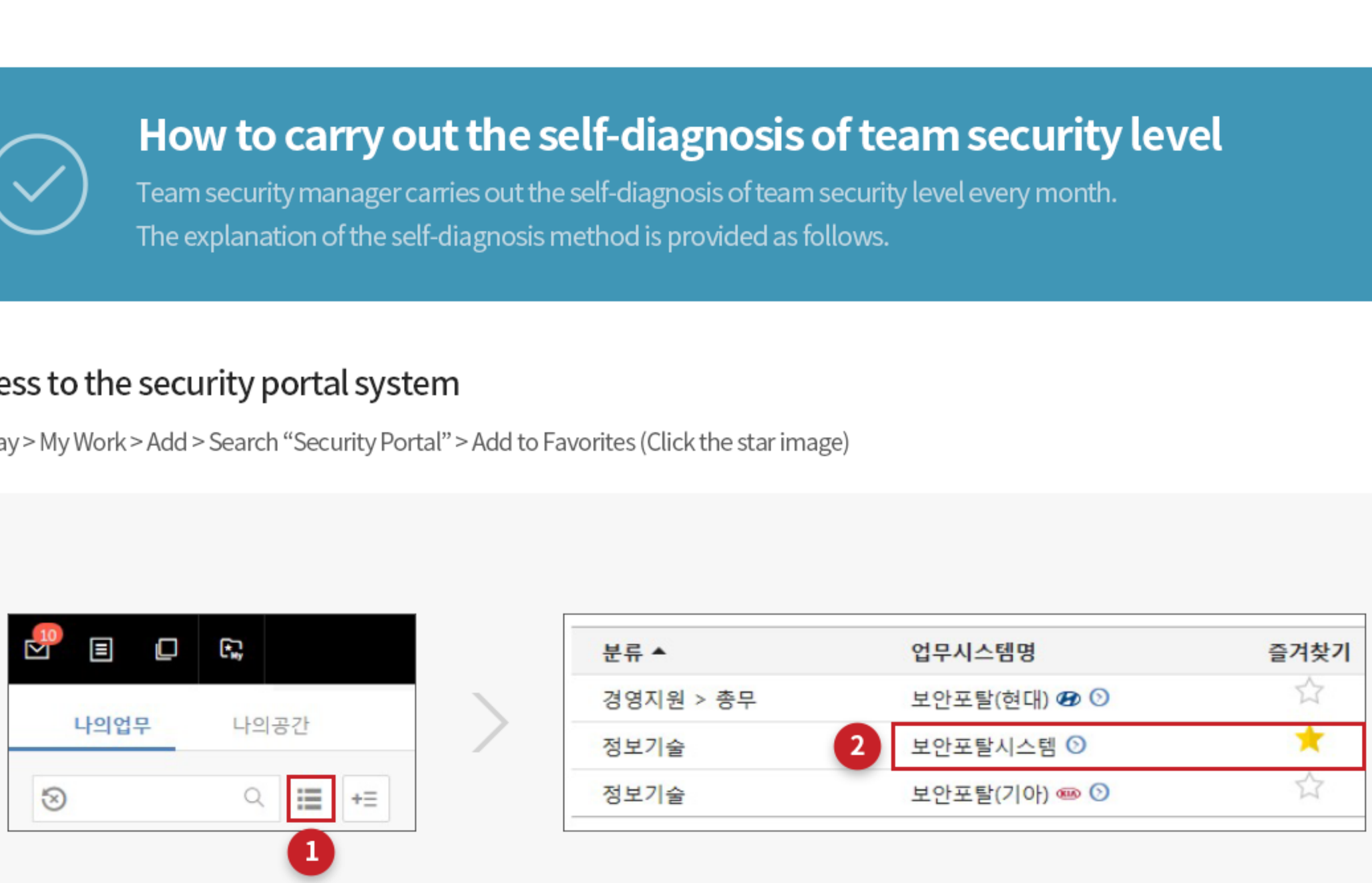
Anyone who is unable to prepare the pledge due to a leave of absence can prepare it after returning to work.

How to carry out the self-diagnosis of team security level

Team security manager carries out the self-diagnosis of team security level every month.
The explanation of the self-diagnosis method is provided as follows.

① Access to the security portal system

- Auto Way > My Work > Add > Search “Security Portal” > Add to Favorites (Click the star image)



② Access to the Self-Diagnosis of Team Security Level screen

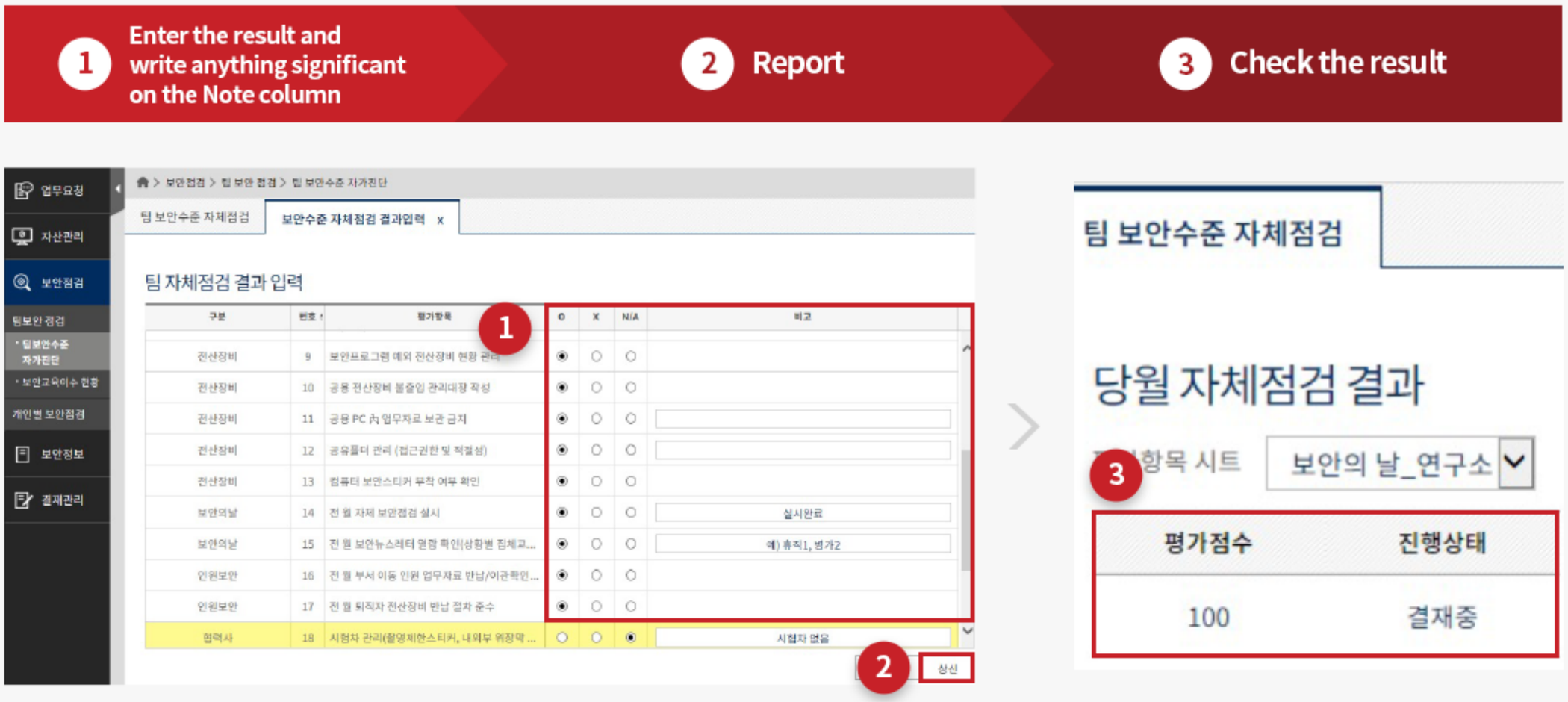
- Cary out self-diagnosis evaluation through ‘Security Inspection’ > Team Security Inspection > Self-Diagnosis of Team Security Level > Enter The Self-Inspection Result of the Team from the menu on the left.

1 Access the List screenzzv

2 Carry out the self-diagnosis evaluation

③ Carry out the self-diagnosis evaluation of team security level

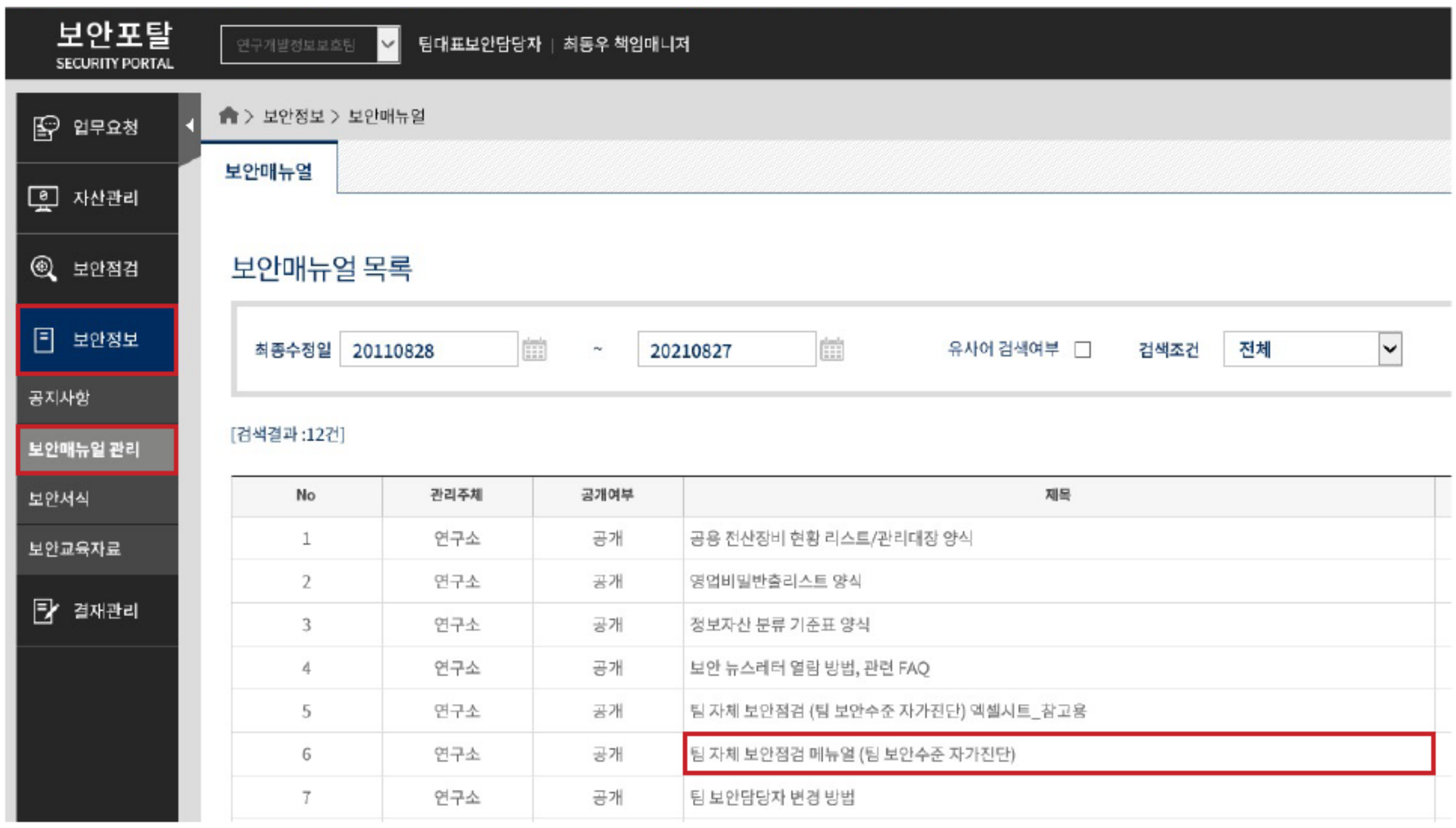
- Make a choice between O, X and N/A according to each evaluation item, write the Note for anything significant and report
- When you report, an approval request mail and the relevant link will be sent to the department head. (Access the security portal through the link or directly and carry out the approval procedure)



FAQ

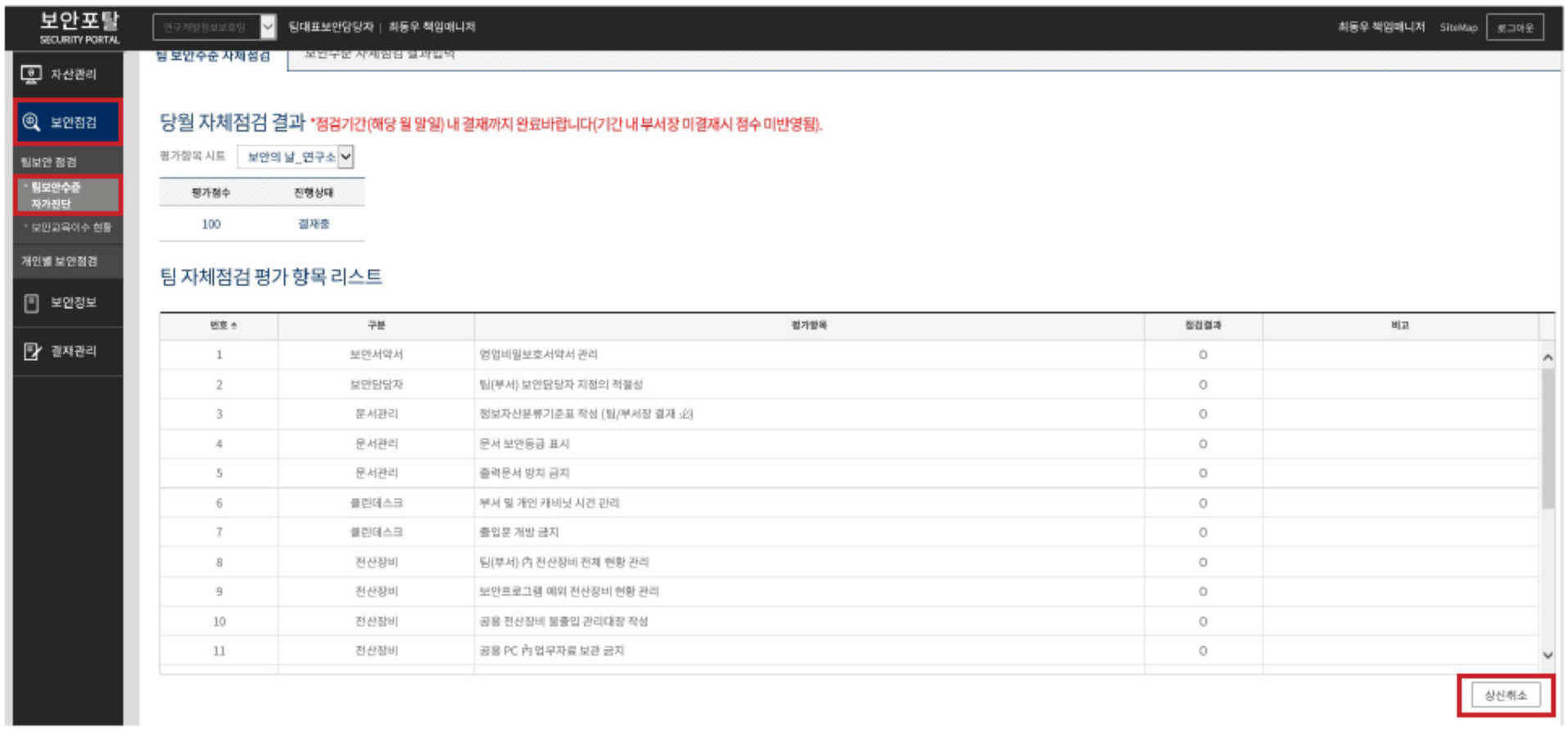
Q1. Where can I view the manual for the self-diagnosis of team security level?

You can view it from the Security Portal. Access the Security Portal and Click Security Information > Security Manual Management > ‘Manual for the self-diagnosis of the team' (Self-diagnosis of team security level)’ from the menu on the left



Q2. It is necessary to modify the inspection details. How can I do it?

It is possible to cancel Reporting and re-enter the contents before it is approved by the team manager.
However, after it is approved by the team manager, it cannot be modified.



Q3. The approval procedure is unavailable due to the team manager's absence. How can I request for the designation of an alternative approver?

You can contact the system administrator and request for the designation of an alternative approver.

How to prepare the information asset classification standard sheet

Information asset classification standard table is the table that shows the type of trade secrets handled by the team (department)\
and their corresponding security level.

사내한

정보자산(문서) 분류기준표

극: 극비, 비: 비밀, 사: 사내한

■ 팀명 : 0000팀　　■ 담당자 : 000

■ 마지막 업데이트 날짜 : 0000년 00월 00일

팀(부서) 취급 보안문서 목록

1. 일반자료

보안문서 목록	보안등급	비고
최고경영층 보고자료		
업무실적 및 업무계획		
업무표준/기술표준		
중장기개발계획(신차/인사/조직/투자 등)		
·		
·		
·		

2. 기술자료

보안문서 목록	보안등급	비고
LRCP		
LRPP / PTCC (연구소 검토용)		
MS/ES		

< SAMPLE >

How to prepare the information asset classification standard table

① Download and prepare the sample form. ※ How to download the form : Access Security Portal → Click Security Manual on the Main screen

② List trade secrets handled by your team by general/technical data.
- Prepare the form for each task and refer to ‘Security Management for Technical Data of Research Institute (HR-EB-CM-075)’ registered on the Work Standards.

③ Write the security level for each trade secret.
- The security level of technical data presented in ‘Security Management for Technical Data of Research Institute (HR-EB-CM-075)’ outlines standard security levels reviewed for each center, and classifies the security level of trade secrets handled by each team by referring to the relevant levels.
- Records data handled by the team, if present, besides technical data registered on the Work Standards.
- Technical data received from other teams should be managed according to the security level set by the team that created such data.

④ After completing the preparation of the table, report it to the team manager through Smart Report, save and manage such table on the team security manager's PC.

⑤ If there is an updated item in the information asset classification table, please apply it to the table immediately and update the table at least once a year.

Roles of the team security manager

Team (department) security manager takes charge of security tasks in the team.

The team security officer is the team manager, and “plays the role of ensuring security management in the team including classification and management of security documents, reception and management of security pledges, management of team security status, team security inspection”.

- Classifies and manages team security documents and team security pledges.
- Carries out the inspection of security in the team and reports the result to the security manager (department head).
- The status of information assets in the security portal system and the asset management register should be maintained and managed properly.

‘Security Organization Composition and Management Procedure ' in the contents of Work Standards

Only one representative security manager (official) in the team can be designated by the authority of the department head.
The permission to carry out the self-diagnosis of team security level is granted only to the team security personnel.
※ For how to designate and change the team security manager, refer to manual.

Team security manager basically carries out the self-diagnosis of team security level regularly.
Refer to the manual regarding how to carry out self-diagnosis of team security level in order to carry out the self-diagnosis properly.
Also, the security education is carried out every year targeting team security personnel. Please participate in the education by referring to this information. (Information is provided through an official letter at the beginning of each year)

How to change the team security manager

Representative team/ department security manager	1 manager	Team security manager	2 managers (More than 2 managers are possible if necessary)

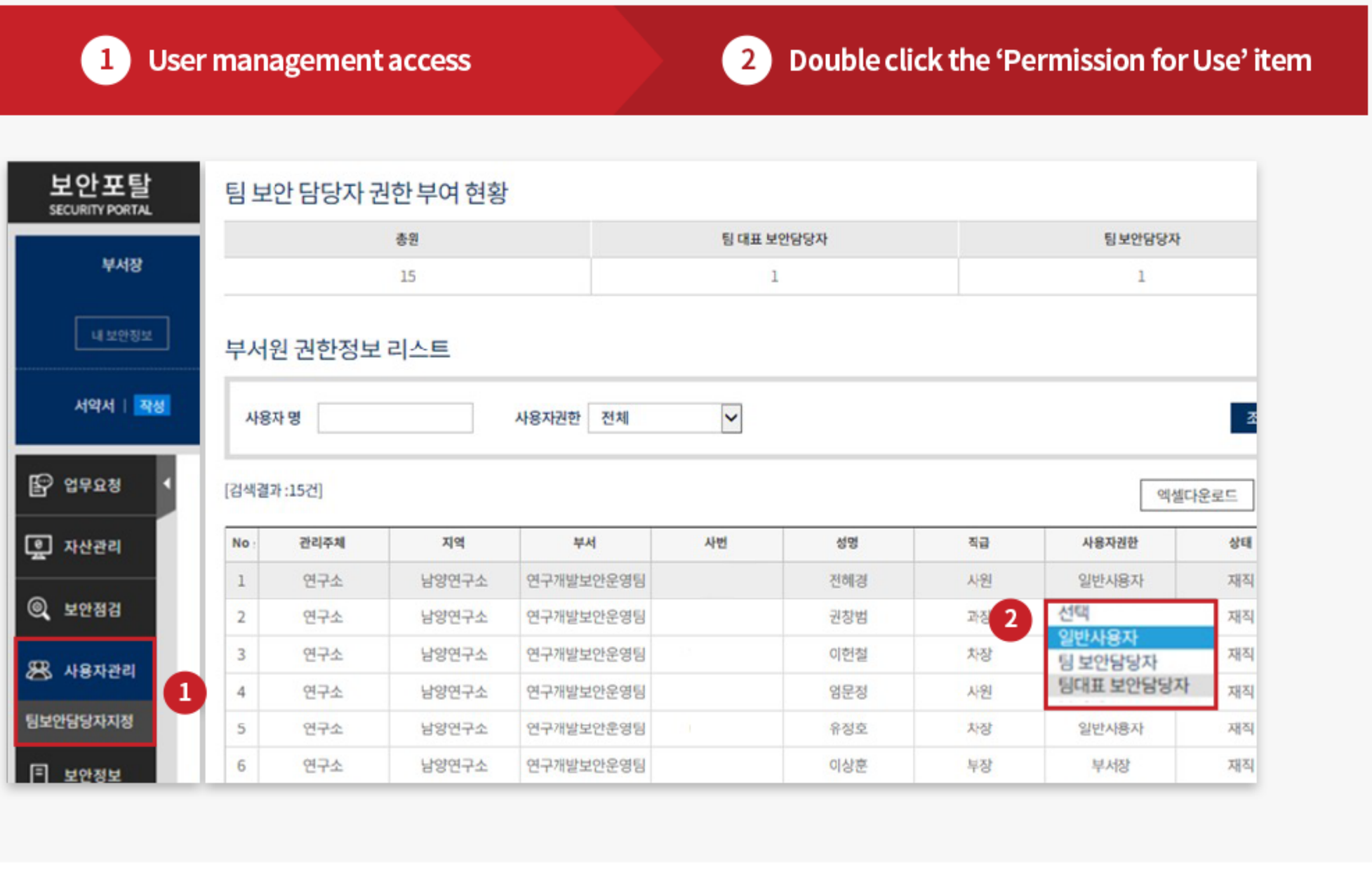
The manager can be changed by the team manager/department head on the security portal, and a person who has worked in the relevant team for at least 2 years or longer is recommended for the security manager. Self-diagnosis of team security level can be performed only by the representative team security manager.

① Access to the security portal system

- Auto Way > My Work > Add > Search “Security Portal” > Add to Favorites (Click the star image)

② Designation or change of the team security manager (Department Head's permission)

- Access Security Portal > ‘User management’ from the menu on the left > Designate the team security manager

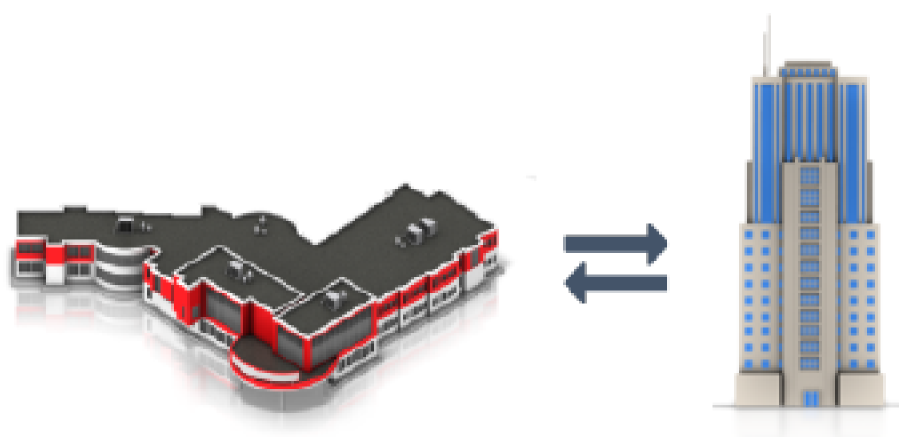


Work data transfer procedure at the time of dispatch/transfer (including computer systems)

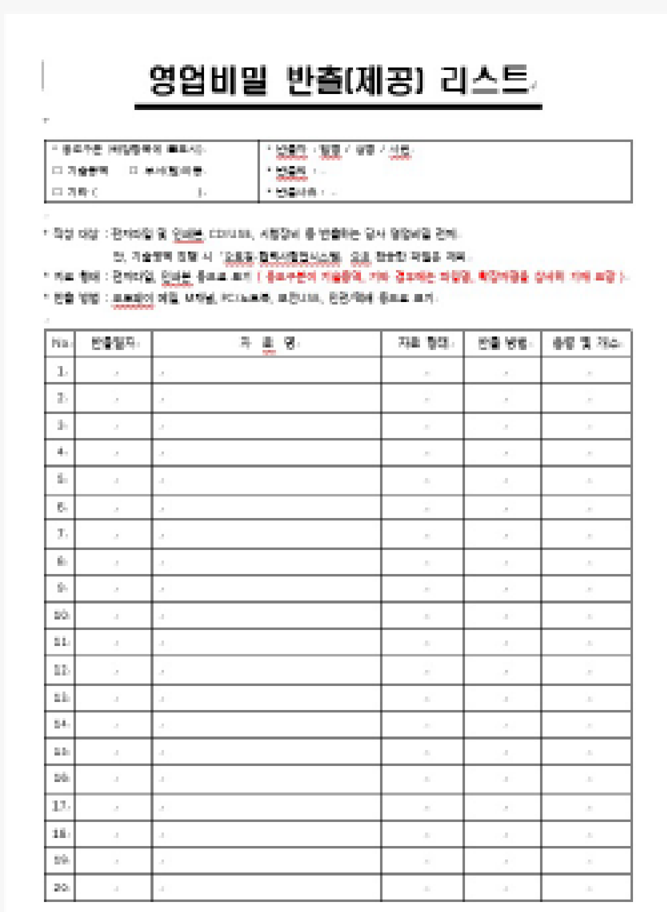
The information on the procedure for transferring PC and work data due to change of team(department) or place of duty is provided as follows.

Computer equipment and work data transfer procedure at the time of dispatch/transfer

1. Team responsible for the return and transfer of equipment : R&D General Affairs Operation Team (PC, laptop computer) / PLM Promotion Team (PWS, EWS)
2. Besides dispatch/transfer between teams, this regulation also applies to the new appointment of an overseas resident employee.

<table>
<tr><th>Classification</th><th>Return/relocate PC</th><th>Transfer of business material and data</th></tr>
<tr><td> 
Transfer to a research institute
(Namyang/Uiwang/Mabuk/Samsung)</td><td>Transfer of PC (bring it along)</td><td rowspan="2">When transferring between teams (divisions), all business materials should be returned to the previous team/ If necessary, prepare ‘list of trade secrets take out' and receive approval from the team manager and have the previous team store it → Send data through Autoway mail, M-channel. (※ However, overseas resident employees should use the overseas resident employee data transmission system.,)
※ ‘Download the form of list of trade secrets take out: Resource</td></tr>
<tr><td> 
Move to other area
(Yangjae, Ulsan, Group, Kia, etc.)</td><td>Return PC (Receive it from the new post)
※For PWS, it can be transferred after consultation.</td></tr>
</table>

Trade secret export (provided) list



영업비밀 반출(제공) 리스트

No.	반출일자	자 료 명	자료 형태	반출 방법	용량 및 개수
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

Research institute's computer equipment take out procedure (Uiwang/Mabuk, PWS, etc.)

STEP 1	Prepare the certificate of free take out and receive approval.
STEP 2	Send it before taking out computer equipment (approval of the team manager) - Contents of official letter: Equipment information, date of movement/location, status of data deletion - All data should be deleted completely and if not, it should be decided by the department head. - Attachment of official letter: Certificate of complete deletion (issued by PC/PWS maintenance office), list of trade secrets take out/provision (Prepare it when transferring work data, refer to the resource for the form)
STEP 3	When you exit the gate, attach a security sticker to the power port and have a security guard check when you enter the gate ※ For factories, the security sticker is checked by the team security manager (Sends the contents checked to the R&D Information Protection Team: Arrival time / location of sticker attachment / number of items, etc.)

FAQ

Q1. Should I follow PC and data transfer procedure just as normal transfer when I transfer to overseas as an overseas resident employee?

An overseas resident employee is also a type of transfer, so please prepare the lists of trade secrets taking out through the data transfer procedure. For PC, follow the guidelines given by the operation division.

Q2. Should I follow PC and data transfer procedure just as normal transfer when I transfer to overseas as an overseas resident employee?

Consult the relevant operation team (PC : R&D General Affairs Operation Team, PWS : PLM Promotion Team) for equipment.

Matters of security to be observed at the time of retirement

At the time of retirement, the employee should return all materials related to his/her work and company to the company and should not hold copies in any form regarding such materials personally.
The followings are the matters of security to be observed at the time of retirement in addition to work materials.

Matters of security to be observed by a retiring employee

① Inform the relevant department of the fact at least 2 weeks prior to the expected final day of work for smooth retirement process.

- Division in charge of retirement process: R&D Personnel Operation Team

- Division in charge of computer systems: R&D General Affairs Operation Team (※ Division in charge of PWS system: Research Institute Technology and System Team)

Division in charge of security work: R&D Information Protection Team

② Matters of security to be observed

- Transfer materials to an employee in the team who will take over the duty
- Return all computer systems including PC/PWS/USB used by (including all work materials related to the company)

※ Return all work data except for personal data (photo, music, etc.) without deleting them

- Take out personal files (photo, music, etc.) using a secure USB under the supervision of the team security manager
- Return mobile OTP and employee ID card, etc. to the relevant team respectively.

FAQ

Q1. How can I take out materials used personally at the time of retirement ?

You can take out personal data (photo, Internet data, personal files, etc.) using a secure USB after the security is reviewed by the team security manager.

Q2. What should I do with company PC and data used personally at the time of retirement ?

· At the time of retirement, all company work data stored by an individual should transferred to the successor and it is prohibited to delete or format company data arbitrarily except for personal data.
· Such data can be returned to the PC/PWS operation team by the person in charge of security or computing in the team.
(Be careful not to format/delete equipment used by a retired employee arbitrarily or not to allow another staff member to use such equipment)

Resident employee's data transfer procedure

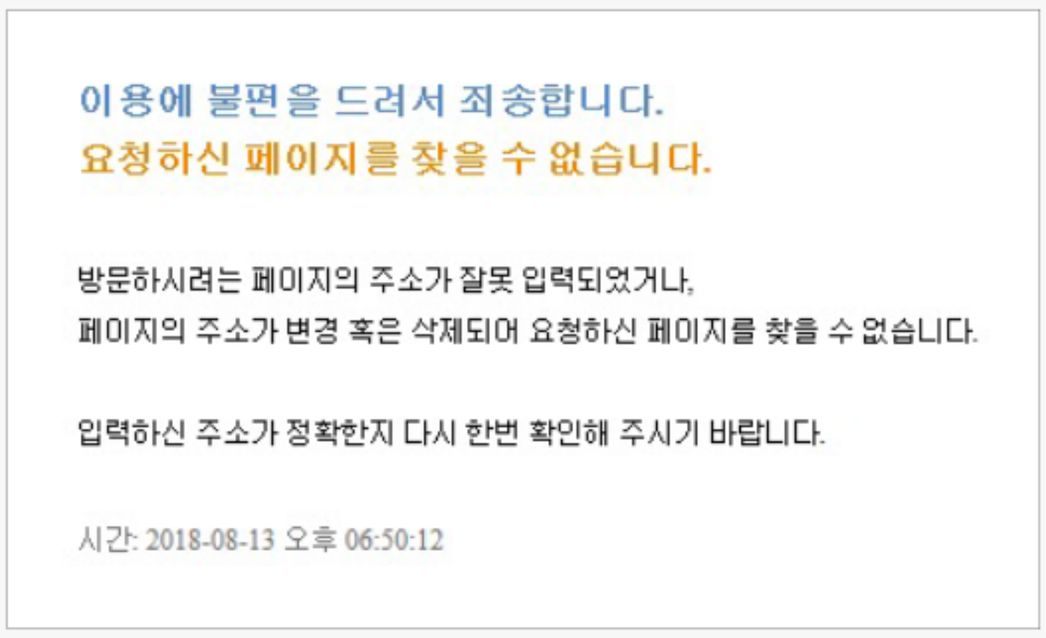
When an overseas resident employee goes to his/her appointed overseas post or returns to his/her domestic post, work data should be returned to his/her previous team. However, if necessary for business purposes, data transfer according to the regular procedure (Use of resident employee's data transmission system) is available.

Procedure to apply for and use the overseas resident employee data transmission system

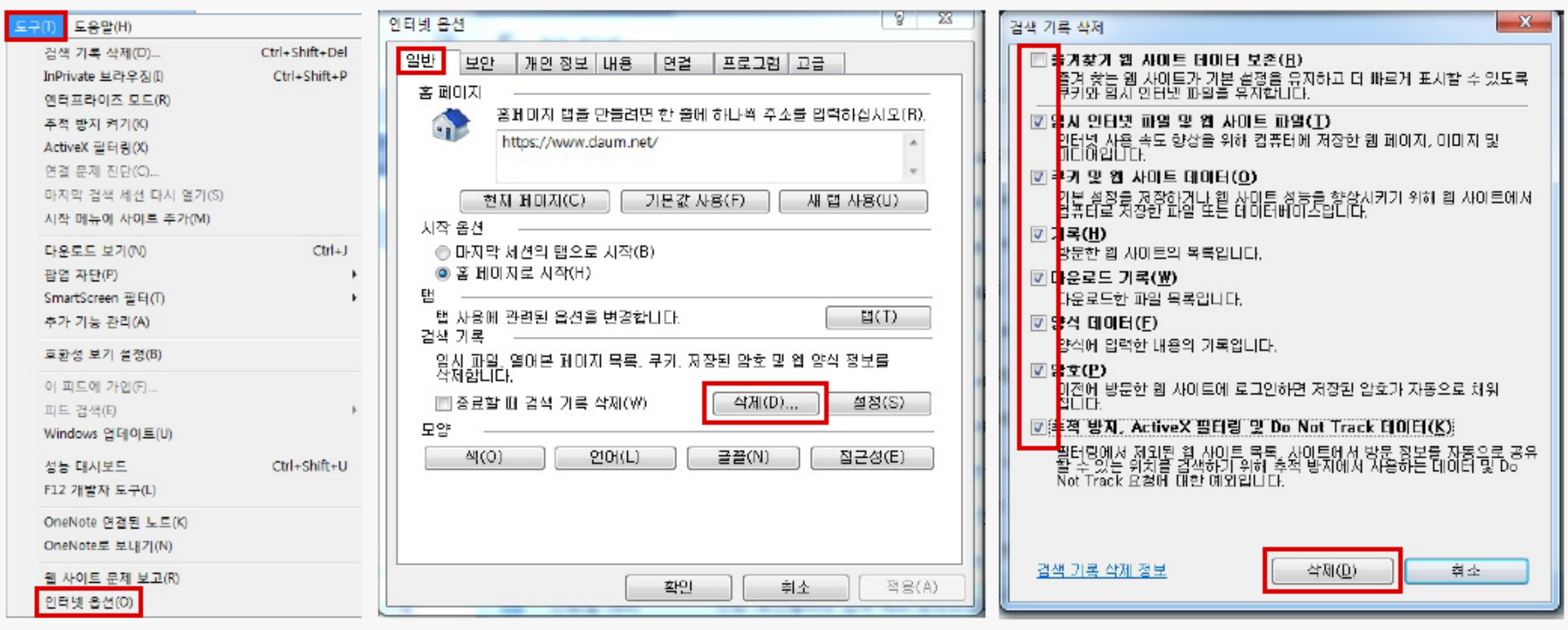
Apply for the system use from SRMS	>	Approve	>	Log into the system and register data to be transferred/	>	The team manager's approval	>	Login to the system from the new place of work and download data.
5-2 Delivery of an overseas resident employee's data and application for in-company Webhard		A notice of approval is sent by e-mail.		https://isecuhard.hyundai.com				

① If a message saying "The page you requested cannot be found" appears when you access the overseas resident employee data transmission system

1) Screen shown when accessing https://iseuhard.hyundai.com



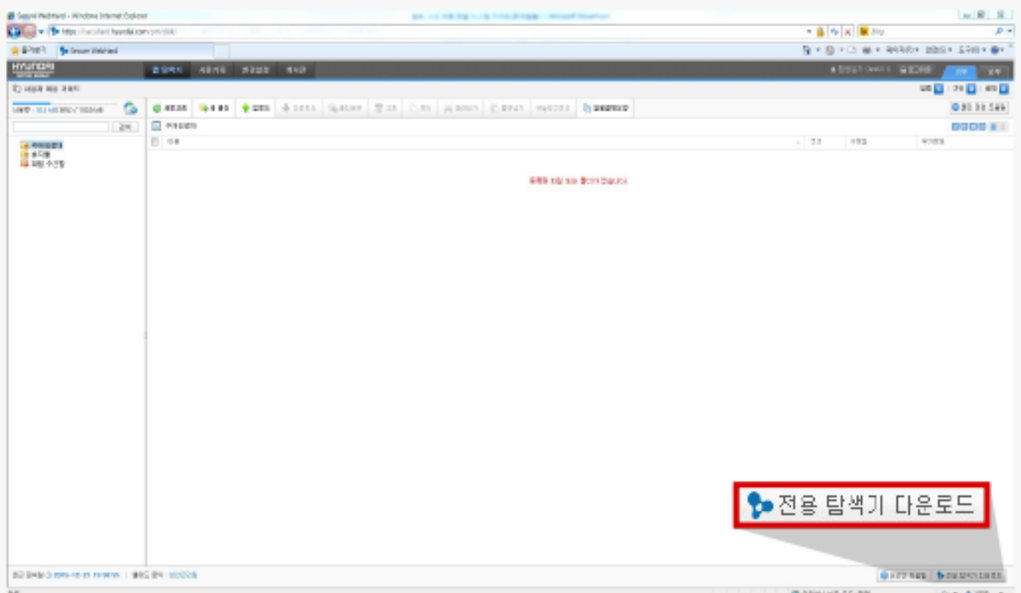
2) [IE menu] Click Tools → Internet Options → General tab → 'Delete' button → Remove a check mark from 'Save Favorites Website Data', put a check mark on all other remaining items and press 'Delete'.

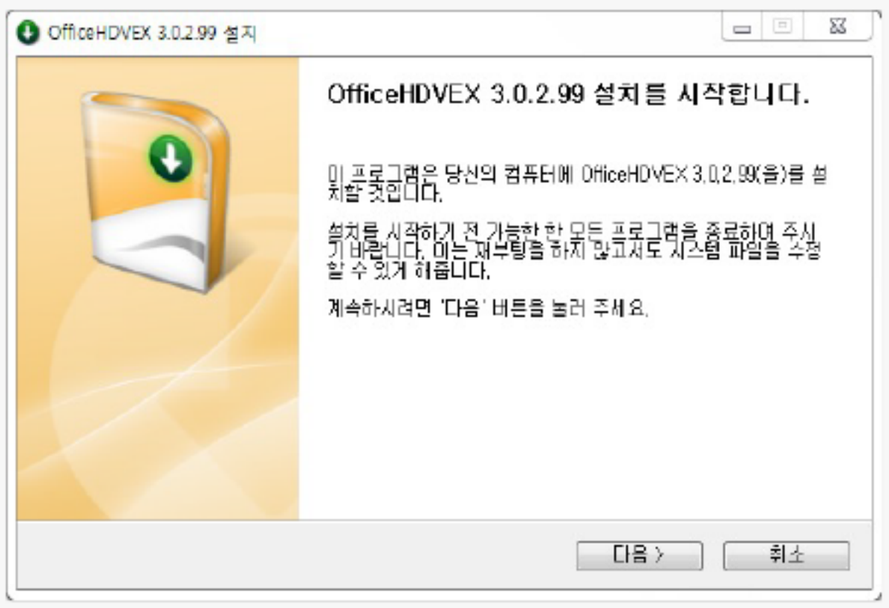


② How to use the overseas resident employee data transmission system (detailed)

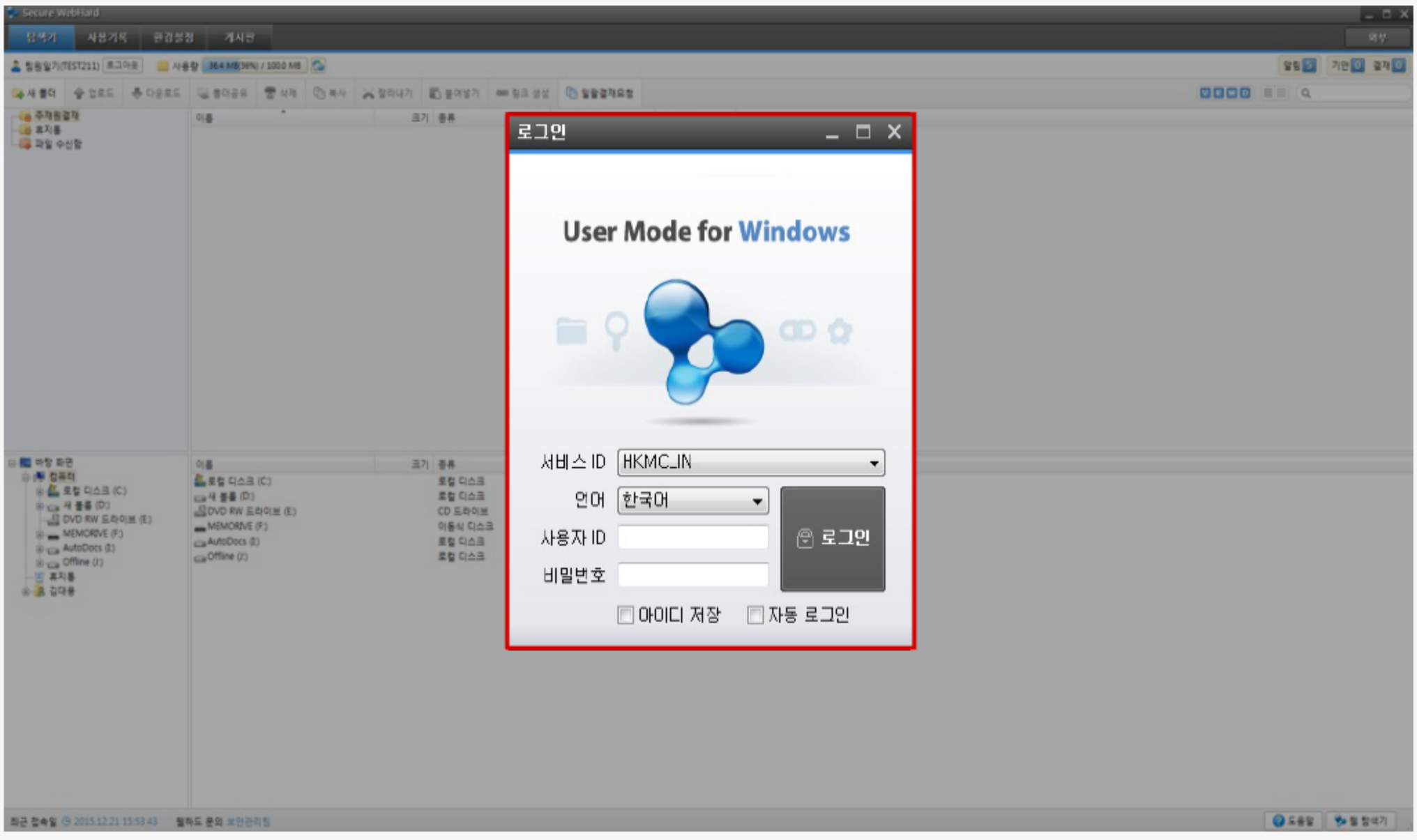
1) After receiving an e-mail regarding the information on application and approval, access https://iseuhard.hyundai.com.

2) Click the "Download Explorer" at the bottom right side of the website to begin downloading (install the program according to the guidance)

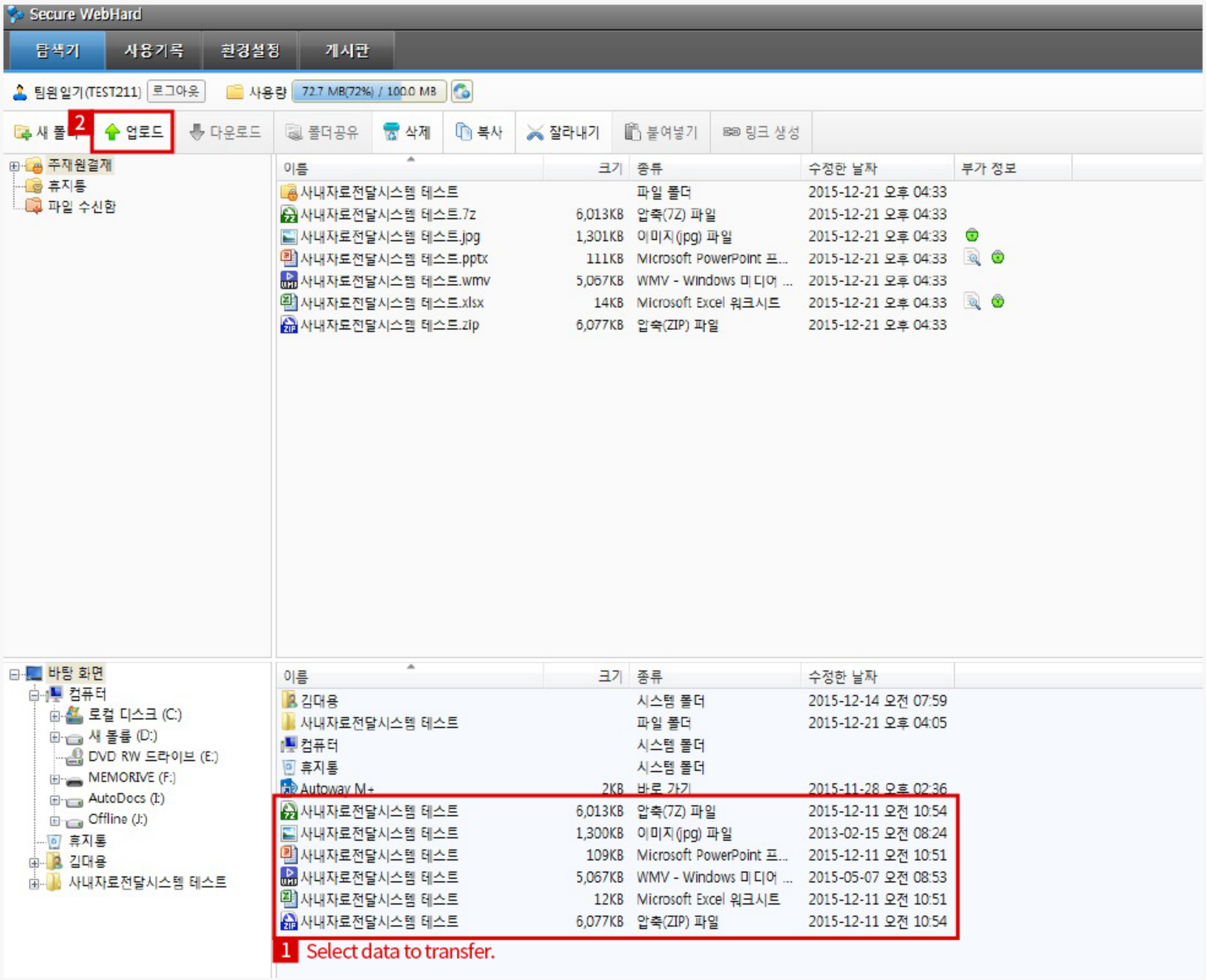




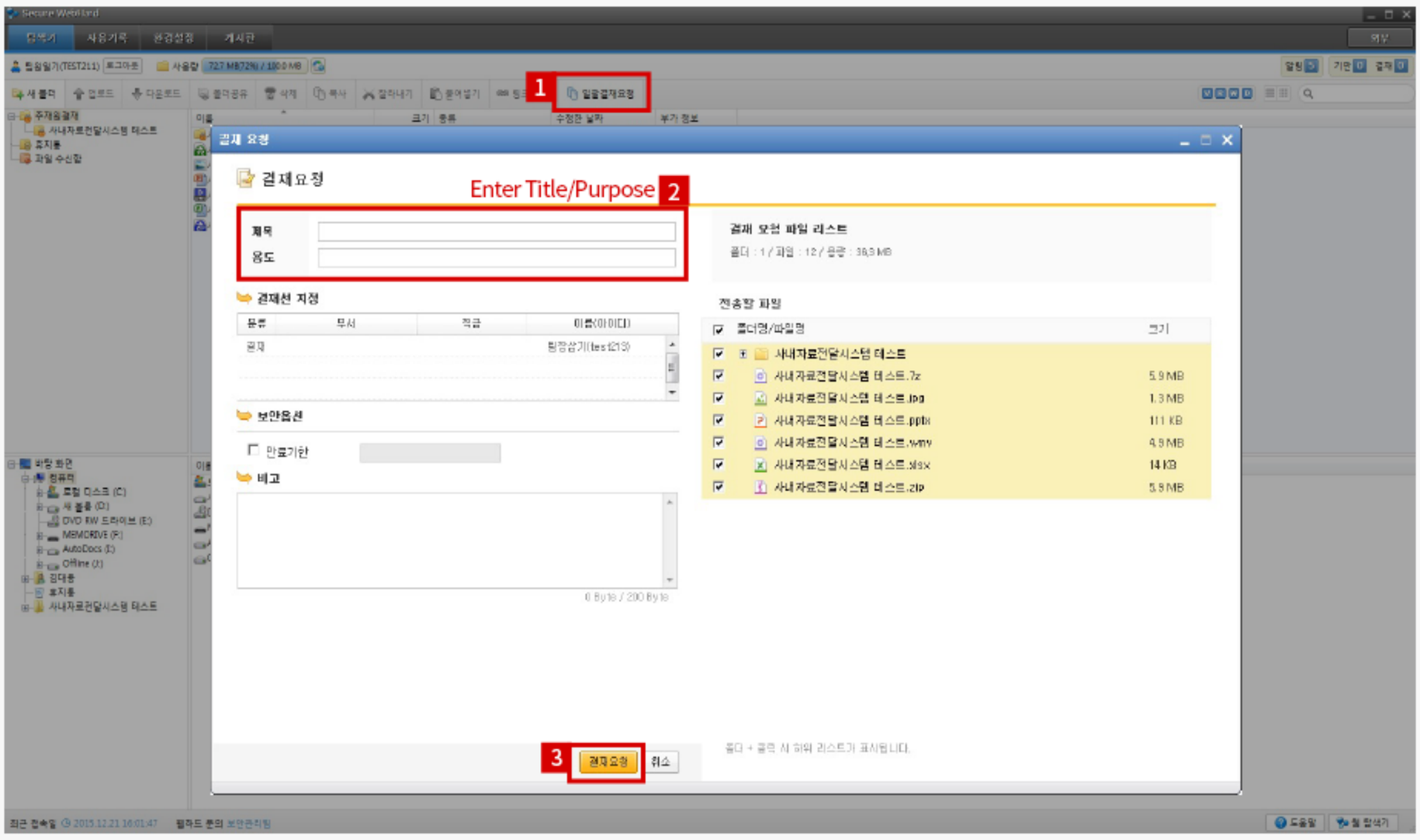
3) Enter Autoway ID/PS and log in



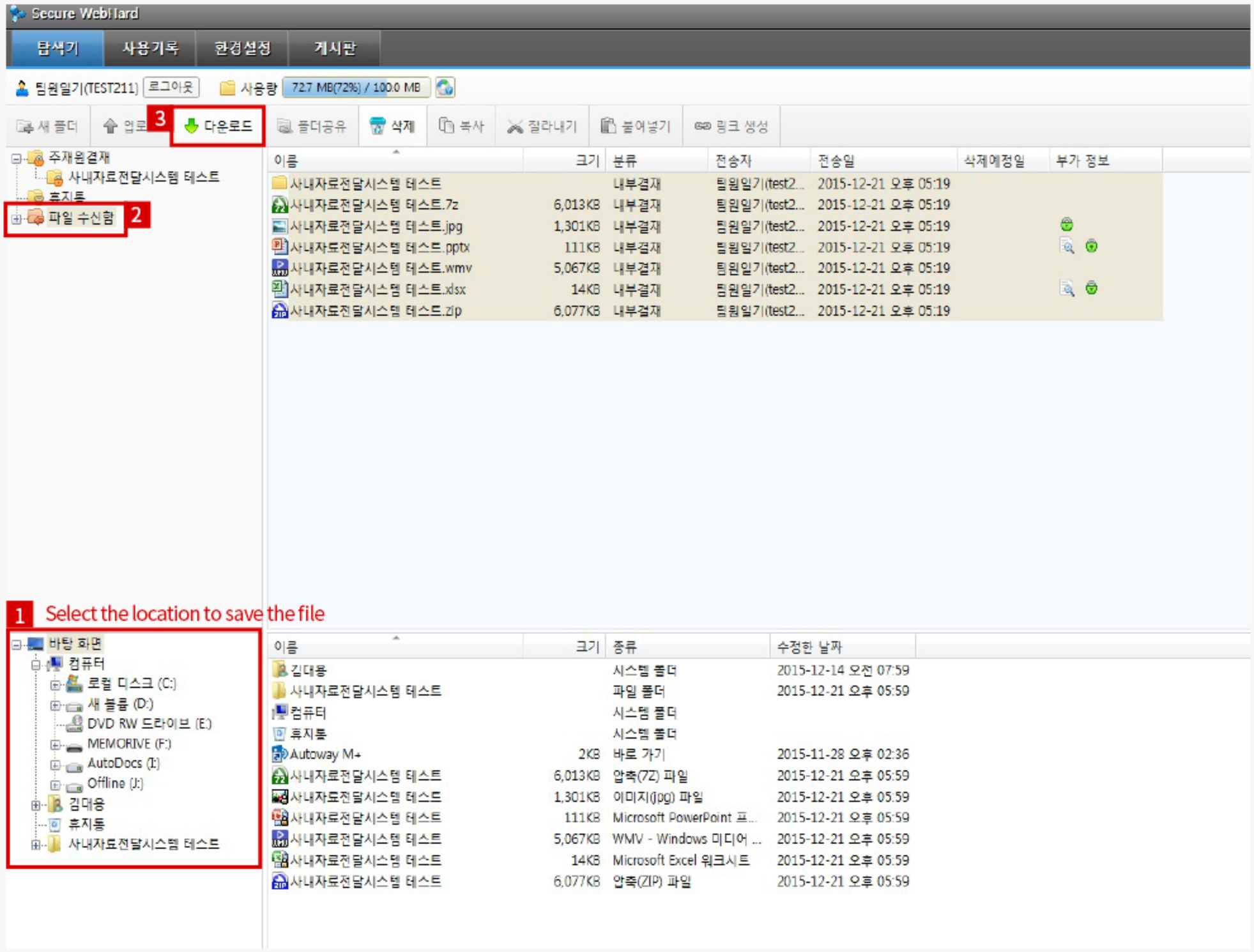
4) Select a file from the local drive and click the “Upload” button or drag and drop the file.
> Compressed files cannot be uploaded (It should be updated in form of file or folder)



5) After uploading the file, click "Request for All Approval” → Enter the title/purpose → Click “Request for Approval”



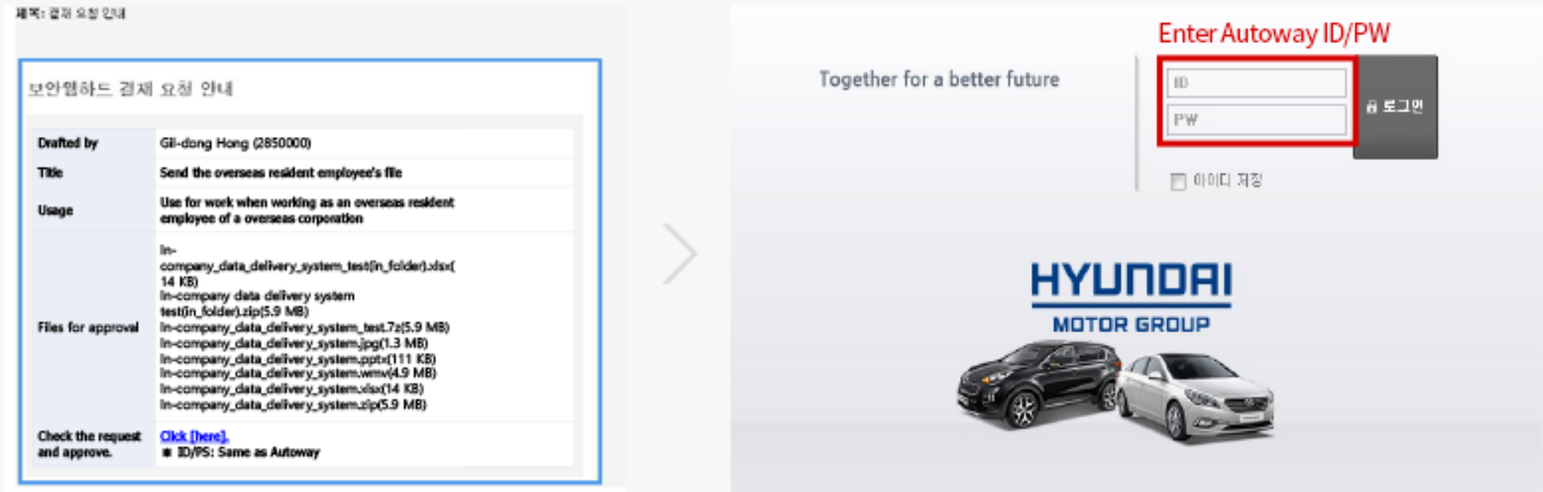
6) After the team manager's approval is received, log into the system at the new post (carry out the same procedure as shown in the previous page) and download data.



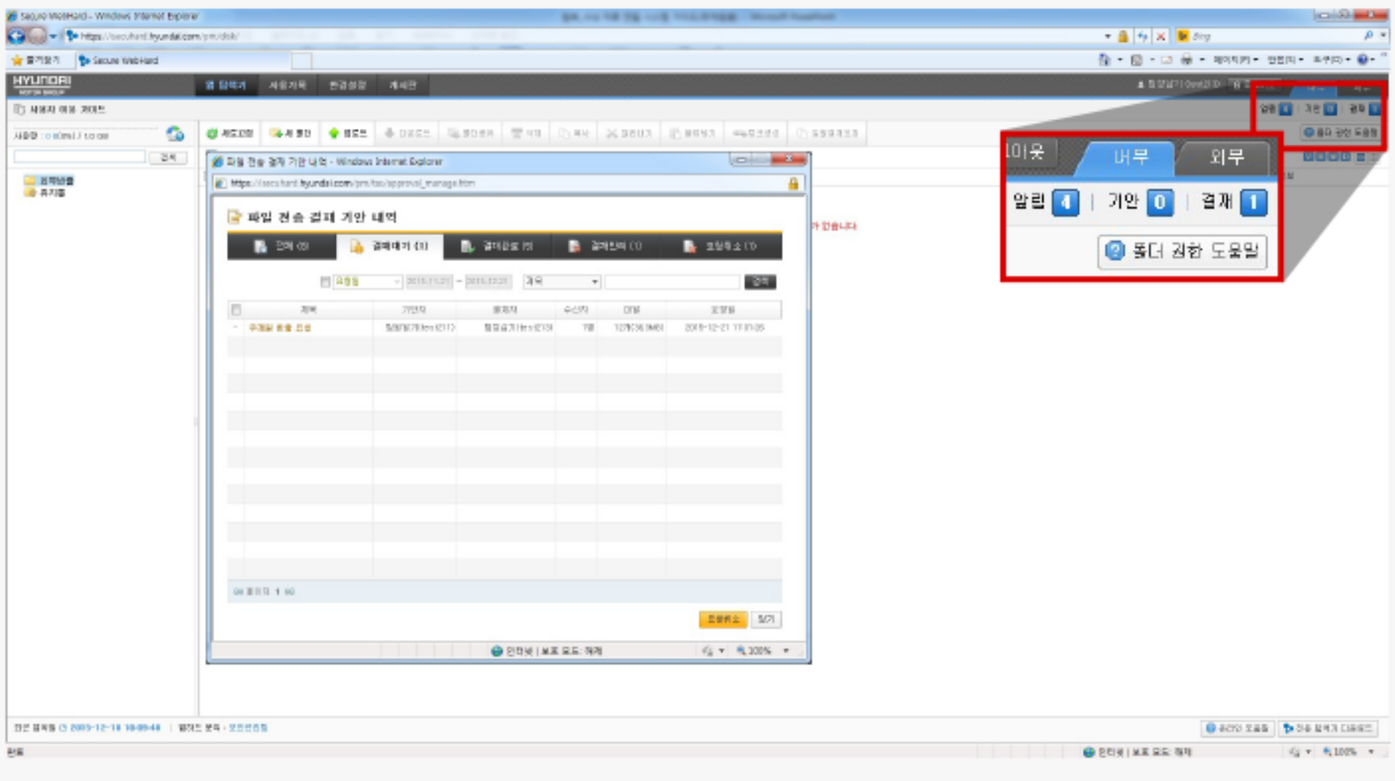
7) After receiving the file, inform the person in charge in the R&D Security Operation Team of the completion of file reception by e-mail (Staff member Jeon Hye-gyeong)

③ How to approve by the team manager (detailed)

1) After checking an e-mail requesting for approval from the Autoway mailbox, click the following link to access the system (https://iseuhard.hyundai.com)

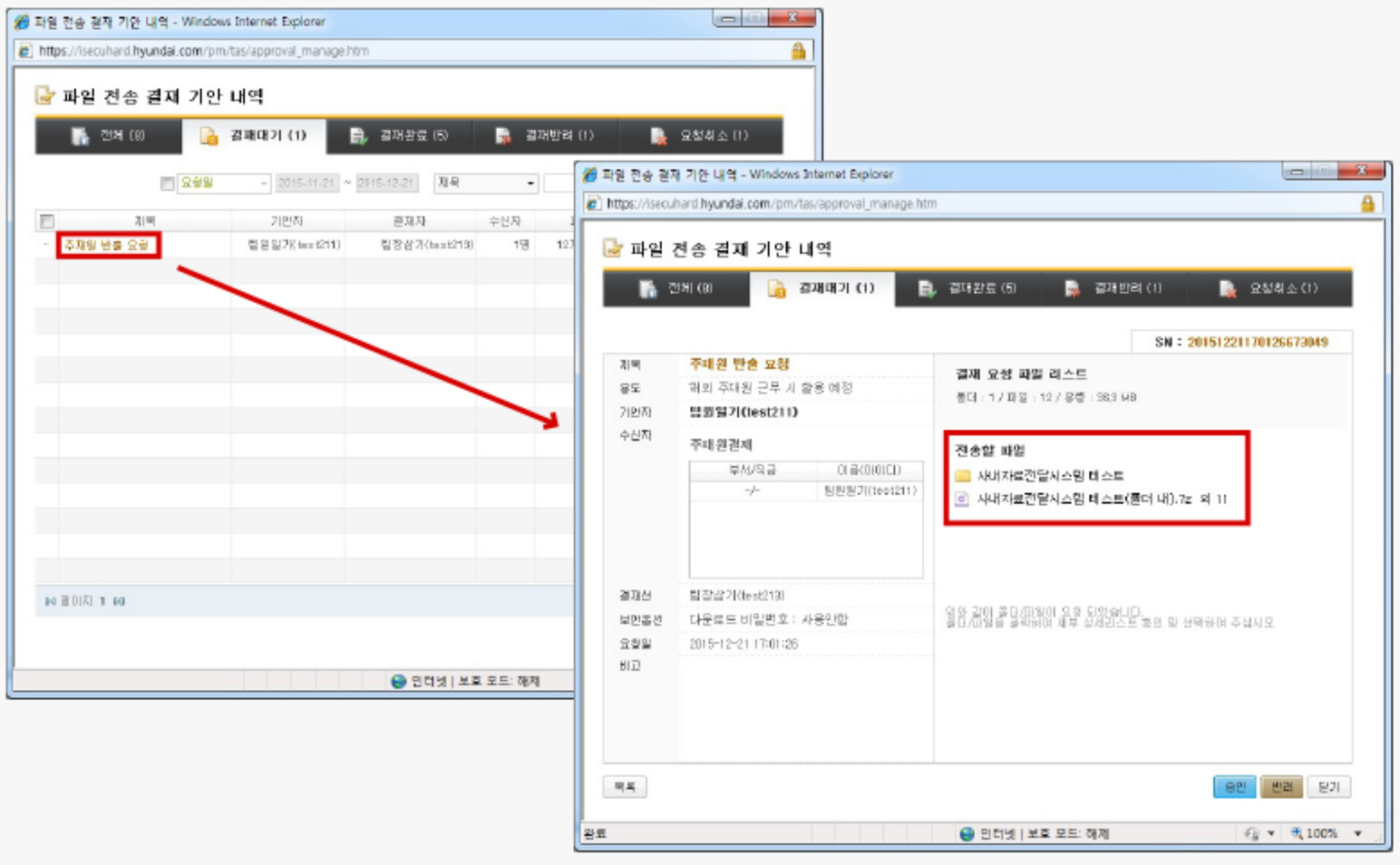


2) After logging in, the approval stand-by pop-up window will appear automatically.
If a pop-up window does not appear, click the Approval button at the top right side of the website.

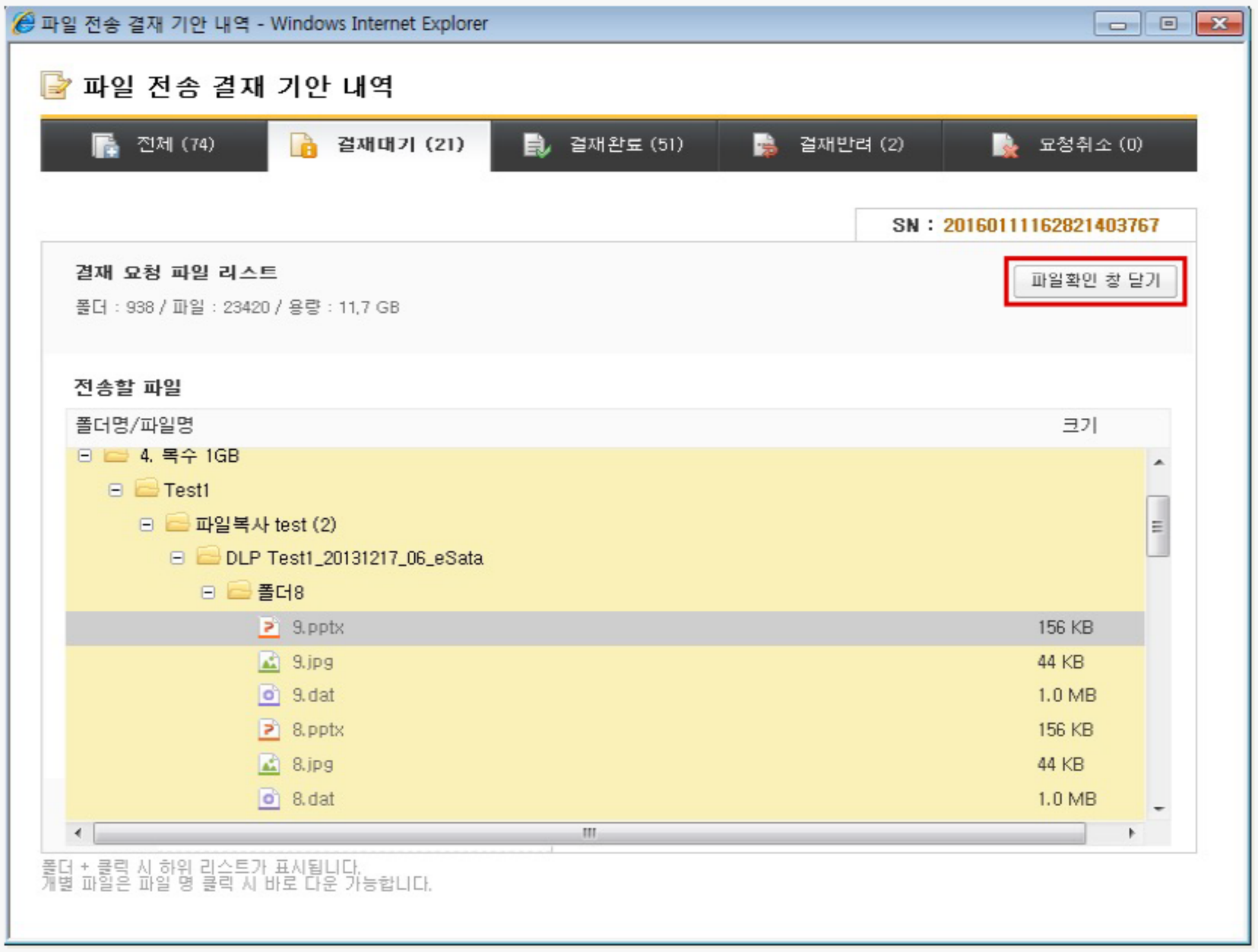


3) When you click a document standing by for approval, a detailed plan pop-up window will appear.
※ If there are a large number of files or the file size is large, it takes time to wait in the pop-up window.

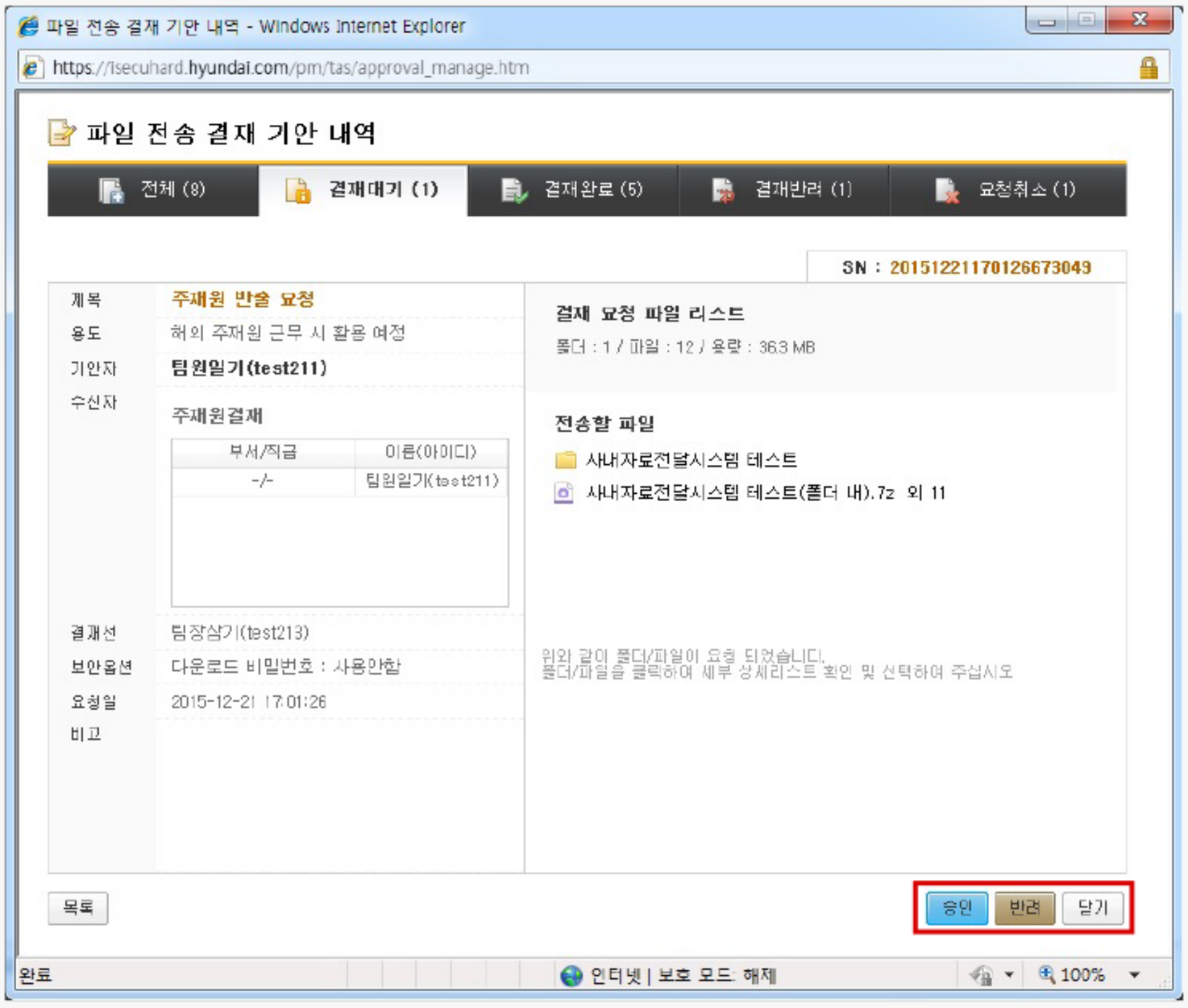
4) Click 'File to send' to check the data to be sent.



5) You can view the contents of the file by clicking the file name. After checking the contents, click ‘Close file confirmation window’



6) When you click ‘Approve’, the approval procedure will be completed and the overseas resident employee can download the files.



How to collect the security pledge from a partner company

When conducting business with a partner company, the security pledge is collected to provide security precautions for conducting business and it should be used as documentary evidence in order to receive legal protection when a security accident occurs. Since the procedure to collect the security pledge varies by company, please refer to the following information.

How to collect the security pledge from each partner company

1st parts supplier (manufacturer)	Since the purchasing department in the main office receives the security pledge when concluding a contract, there is no need to collect it separately in the field.
Technical service	When preparing my contract from ROMS, attach the security pledge and submit it together.
Others	Receive the security pledge separately. ※ Download the form : Resource

FAQ

Q1. Where can I download the form of the security pledge for the partner company?

Resource → Download the standard security pledge for partner companies (for CEO/for executives and staff members)
Both the security pledges for the CEO and for executives and staff members should be received.

Q2. Due to the characteristics of the work I carry our with the partner company, the contents of the form of the standard pledge provided should be modified. In this case, what should I do?

If the modification of contents in the provided standard security is necessary, you can do so after requesting the legal team to carry out a review.
※ How to request legal advice from the legal team : Access Autoway - My Work Access 'Legal Support System' → Request for legal advice

Security procedure and matters to be observed for employing a service

Technical service work procedure

Conclusion of a service contract	Have the technical service partner company (representative/person in charge) write the security pledge (In the case of an electronic contract, it is collected via online automatically.) Deliver the security matters to be observed to the partner company. ※ The person in charge in the service promotion team delivers the security matters to be observed (contents of the security pledge, provision of technical data and disposal procedure, etc.) to the person in charge in the partner company at the beginning stage of the service and request for compliance. ※ If the computer system establishment/development is included, it should be reviewed in advance by the relevant department and carried out with the support of technical services or according to the IT investment procedure. (If it is determined that the matter should be performed with the support of technical services, carry out the security review (SAMS) procedure separately,)
Deliver technical data	Deliver data through the 'Partner Collaboration System' (formerly Auto One) (Preparation of 'list of trade secrets take out' is not required) If the partners' collaboration system is not available, deliver materials by Autoway e-mail (CC to the team leader) ※ If both the system and Autoway are not available, data can be delivered through Autoway M+ (avoid using it if possible) However, prepare the 'list of trade secrets take out' (refer to Namyang access security system - security from), report it to the team leader by e-mail and send data. ※ When sending data, notify of security precautions (prohibition of arbitrary distribution/posting, and add a phrase such as our permission if necessary) ※ If a security accident occurs, report it to the R&D information protection team immediately.
End of the service	Return materials or verify the disposal of materials (return technical materials provided by us, service derivatives/products or verify the disposal of such materials) Carry out the disposal check through 'Partner Technical Data Disposal Check System' and return data / Collect a certificate of disposal - Register the certificate onto 'Partner Technical Data Disposal Check System' (Refer to 'Namyang access security system' - Security Regulations) ※ Refer to the Resource for the certificate form ※ Data disposal schedule can be adjusted when the service contract has remaining AS period or in case of additional service.

FAQ

Q1. If the computer system establishment/development is included in the service, why do we need the security check and how should we conduct it?

1) Reason for security review: In the case of building/developing computer systems and IT facilities, measures should be taken in advance to check for vulnerabilities through mock hacking and data should be open to the outside in addition to implementing necessary protective measures in accordance with relevant laws such as the Personal Information Protection Act and Act on Expansion of Dissemination and Promotion of Utilization of Information System.
2) Security review procedure: After prior review conducted by a related department by e-mail, review the system security risk in advance through the Security Review System (SAMS). ※ Related department R&R
① R&D Information Protection Team: Review the security vulnerability for technical service on the computer system and SW development
② R&D Investment Planning Team: When reviewing the technical service plans, confirm the opinion from IT department indicating that it cannot proceed in case of computer system SW development
③ Data Platform Operation Team: Review the technical service plans whether such plans are subject to the targets of information system construction
④ PLM Promotion Team : Review IT infrastructure-related items (server, etc.) within the range of technical service promotion in advance.

Q2. When should the partner use the VDI (virtual PC)?

In order to reinforce the security for key products (models, source, etc.) controlled and developed by our company, the partner should develop, save and share products through a virtual PC installed within the server in our secure network. (Refer to the ROMS message board for details)

- Target control logics for application: Control logics related to national core technologies (ex. fuel cell FCU, electrified BCU, engine/transmission ECU/TCU, autonomous driving logics, etc.) and other important control logics requiring protection as our trade secrets (electronics, chassis, infotainment, etc.) ※ If it is subject to the above regulations, but VDI cannot be used, it is necessary to proceed after consultation. (the matter requiring decision making)

Q3. How do I check the return and disposal of materials provided to the partner company?

1) If there are materials provided by our company to our partner company (including all materials delivered by other methods such as ‘list of trade secrets take out + sending by 'Partner Collaboration System’ and printing), request return of all the provided materials and confirmation of disposal.

2) If data is delivered through 'Partner Collaboration System’, carry out the disposal check through ‘Partner Technical Data Disposal Check System’.
※ Refer to ‘Namyang access security system' - Security Regulations for the detailed manual of ‘Partner's Technical Data Disposal Checking System'.

3) If data is sent to the partner company using Autoway mail, Autoway M+ or other methods, the disposal of such data should be verified based on the ‘List of Trade Secrets Take Out'. (Upload the verification result onto the ‘Partner Collaboration System’)

4) A written confirmation of data return/disposal under the name of the CEO of the partner company should be collected, and if important ‘secret’ or higher level technical data has been delivered, visit the partner company directly and check on the disposal. (Decide the period of disposal check by considering the AS period and the service extension. This regulation does not apply to overseas branch offices.)

Security procedure in case of distribution/publication to the outside such as a paper presentation and a lecture held outside the company

Distribution work procedure to the outside of the company

- When our security document is submitted or distributed outside the company, it should be done after obtaining the approval from the sectional security manager under the responsibility of the team/department security manager.
- Security documents that will be distributed to the press/media are reviewed and distributed by the PR team.

Publication work procedure with regard to the outside of the company

① When publishing a security paper, it is published using a publishing company registered with our company.

② Provide the publishing company with the security document with team manager/department head's approval.

③ After the publication, a request should be made to destroy the security document completely.

Security review procedure

Prepare the application for outside presentation according to the standards of Autoone academic information system (Notice) and obtain approval (academic conferences (inside and outside the company))

- In most cases, even the security review is approved within the academic information system.
- Procedure guide : Autoone → Workspace → Development Support → Academic information system (RIS) → Notice

Send data for individual paper presentations that are not supported by the Autoone academic information system to the R&D information protection team.

- Contents to be include : Attach security review details and application for external presentation..

Security guide for external materials such as external paper presentations and lectures

1. The writer of the paper and the team manager in the relevant department are in charge of preparation and reviewing of the paper and external presentation material.

→ The person who prepared the presentation materials and his/her team manager should take precautions for the level of completion for the materials and not to leak trade secret data.

2. Security guide for preparing papers/external presentation materials

1) Delete all vehicle development / business information items that are not released to the outside of the company

- Vehicle model code, new vehicle release schedule, development cost, business plan, our vehicle development process, etc.
- Cost/weight information, quality issues, applied technologies, production technology, etc.
- Information mentioned in our technical data such as design guide and TDP (standards, procedures, methods, target values, etc.)
- Company organization chart, organization name, manpower operation status/plan, personnel/financial related matters, etc.
- company's know-how and security data of Restricted level or higher

2) Review technical contents (plans) mentioned in paper / external presentation material

- Any information that is not released to the outside should be deleted (Refer to Paragraph 1) above)
  and if it is necessary to talk about technical contents, it should be modified in the form that prevents outsiders including rival companies from using such information.
- Information announced through Internet/news after proper review and approval procedures and publicly known academic information can be used.
- It is okay to disclose the relevant information if it is publicly disclosed to related people by law, national/international standards, etc.
- If the relevant content has been applied for as a patent, it is protected by a patent, so it is okay to be disclosed (write the patent number in the paper).

FAQ

Q1. I'm planning to prepare and announce a paper or a preparation material outside the company and who will carry out the security inspection ?

For an external presentation, your team carries out the security review, and in the case of an in-company academic conference, you can register the security review details on the RIS system, and in the case of a paper or presentation material that will be presented outside the company, you can send such material to the R&D Information Protection team.

Q2. The university intends to present a paper based on the results of the industry-disciplinary project I carried out, and how should I proceed?,

For industry-related projects, the R&D technology strategy team should observe the operation policy.
For security reasons, if NGB forwards the request from the university, please obtain approval from the head of the relevant team and conduct a security review specified in paragraph ① above.

How to Use a Shared folder and Security Precautions

When you need to share data between each user's PC during work, you can use the "Windows Shared Folder" function. However, be sure to observe the following security precautions.

Security precautions for using a shared folder

- Only files that need to be shared for work are used by granting access permission to a limited number of people.
- Be sure to delete the default permission set for everyone previously and set the permission only for the necessary number of people.
- Delete or stop sharing the shared folder whose purpose of use has ended.

FAQ

Q1. How can I set a shared folder?

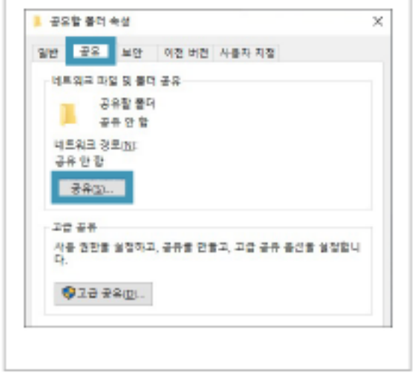
※ Caution

Please set ①~⑨ in the order given in the manual below.

Both settings must be done in order, and if you set only one or set it in the reverse order, there may be a problem with the permissions.

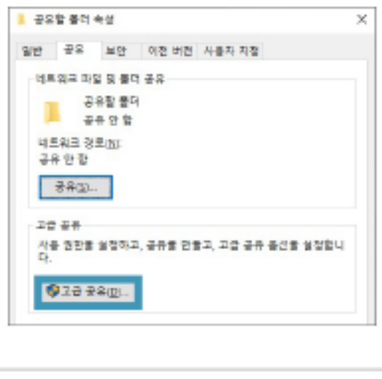
After the initial setting, if you need to modify permissions such as adding or deleting a person, you need to set in the same order including Share → Advance Share to complete correct permission setting.

STEP 1
Right-click the folder you want to share and click 'Properties'.

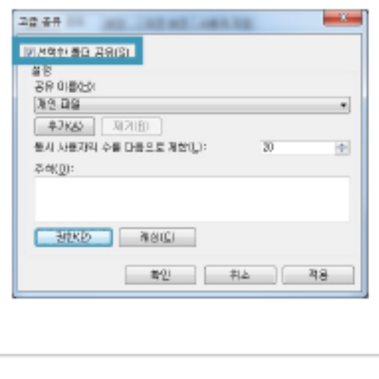


STEP 2
Click 'Share' from the Share tab.

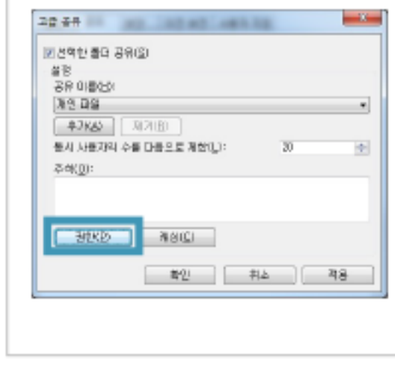
STEP 3
Add the user (company No.), set permissions and click 'Share'.



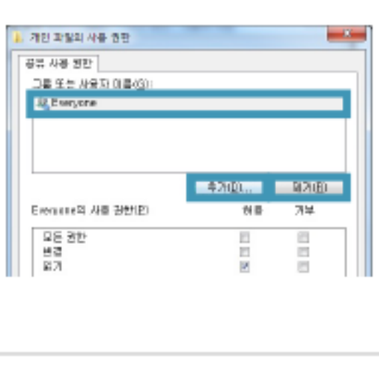
STEP 4
Next, click 'Advanced Share'



STEP 5
Put a check mark on 'Share the selected folder'.

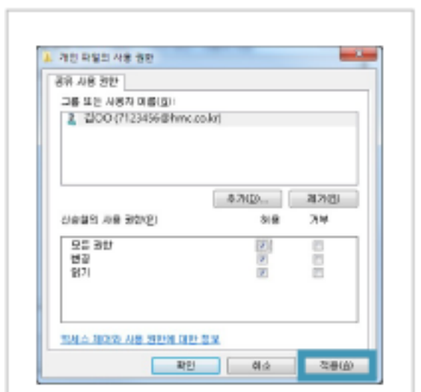


STEP 6
Click Permissions



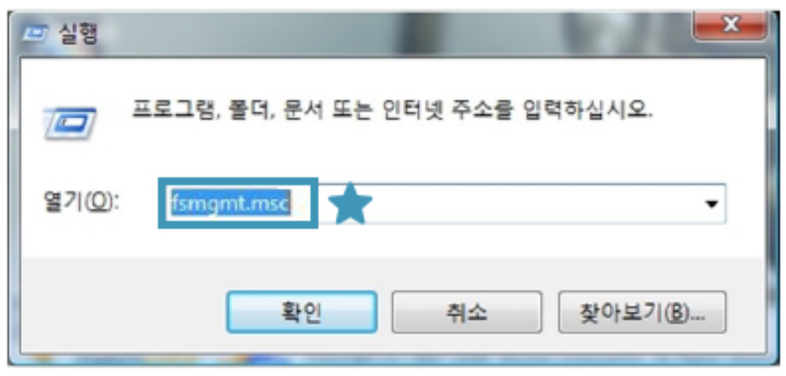
STEP 7
Delete 'Everyone' permissions and click 'Add'.

STEP 8
Add the user (Enter the name or company ID number)



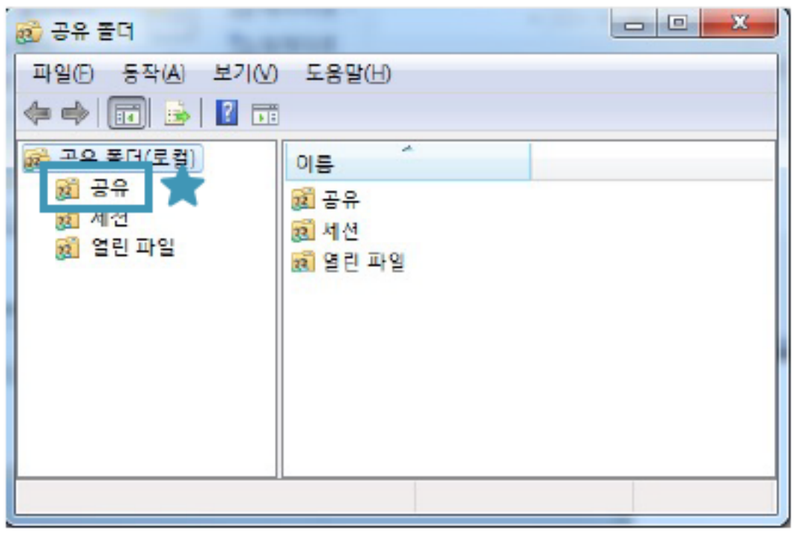
STEP 9
Check if the permission of the added user and everyone has been deleted, and the click 'Apply'.

Q2. How can I verify a shared folder set on my PC?



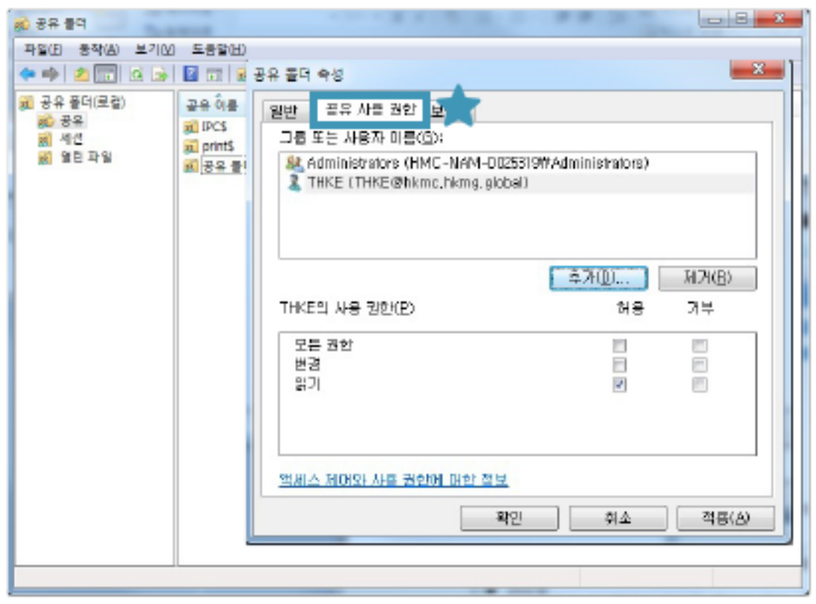
STEP 1

- Open the "Run" window by pressing 'Windows' key and the R key on the keyboard,
- Type ‘fsmgmt.msc’ on the "Run" window and press OK.



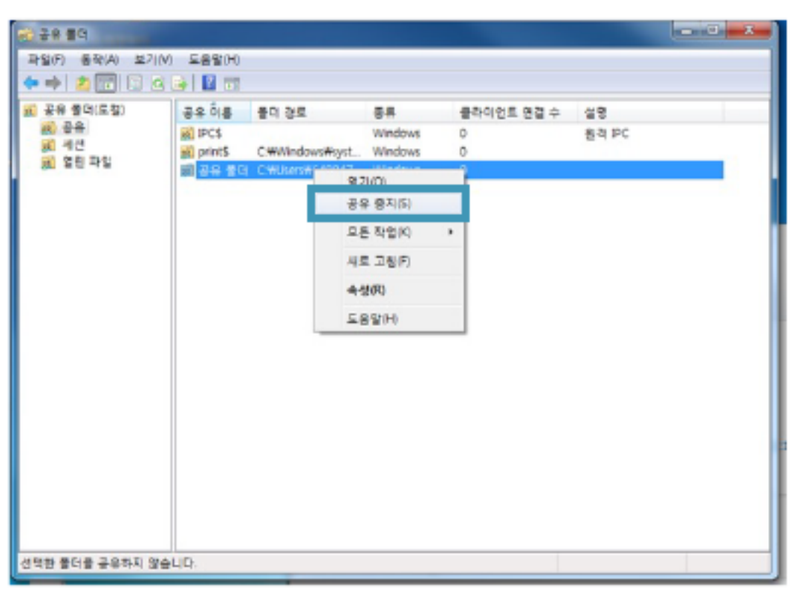
STEP 2

Click 'Shares' shown in the above capture on the window.



STEP 4

- You can view the ‘Properties of a shared folder’ by double clicking the shared folder from the list.
- You can view the permissions of a shared folder from the ‘Permissions to use sharing' tab of the 'Properties of the shared folder' window.



STEP 3

- You can view the whole list of shared folders in the relevant PC.
- You can 'stop Sharing' through the right click menu for each folder

Q3. Can I use a shared folder in order to transfer data from test equipment to PC for business purposes?

Yes, you can. However, be careful of permissions setting when using a shared folder. (Refer to 'How to set the shared folder')

Q4. Can I use a shared folder for sharing the source codes for a vehicle under development with team members?

Yes, you can. However, it is prohibited to share security data in a public PC in the conference room and team code where public accounts are used.

Q5. Can I create a shared folder in idle equipment in the team and share the development guide (ES,MS) managed by the team?

Please manage and use major data related to vehicle development such as specifications and drawings through regular systems such as vehicle development standard system or PLM. It is okay to store and share the data you are currently working on and reference data on a local PC, but please avoid accumulating data that you are not currently using, such as data of old vehicle models, on the local PC for a long period of time.

※ Please refer to the opinion from the data division that since the locally stored data has a different version from the data registered in the system, there is a possibility of problems in vehicle development, so the latest data registered in the system should be used.

HYUNDAI

MOTOR GROUP