22-07-06 JJ V1

Access Policy for the European School of Mol

Reference document.: 2021-09-D-24-en-2 - Access Policy for the European Schools & OSG Guidelin

Table of Contents

1. Purpose

The European School of Mol is committed to providing a safe and secure environment to enhance the personal security and safety of all members of the European School of Mol, while at the same time, protecting the property and privacy of the individuals assigned to use the School's Facilities. The purpose of this Policy is to establish the principles for authorizing, monitoring and controlling access to the schools' Facilities.

2. General context

The global security concept of the European School of Mol is composed of several distinct components in order to create a secure and safe environment for all people present on campus: pupils, school staff, Parents Association members, parents, contractors, visitors, etc.

The development and implementation of access procedures, based on this Access Policy, combined with a proper perimeter security network, will foster a secure and safe environment as described above.

The Access Policy determines the framework in which the school operates to develop effective and efficient access procedures and access control system. The access procedures developed will deal with the following aspects of access security:

- Managing all in- and outgoing persons on the school compound; and
- Managing access to the different areas of the school compound in accordance with predefined access restrictions.

It must be noted that the Access Policy is applicable for all regular entrances to the campus. Improper access to the campus by any other means must be considered as an intrusion and be dealt accordingly.

3. General principles

This Access Policy document is designed as a primary document which contains the basic principles for the access security for the European School of Mol. The concept is based on the Access policy for the European schools and OSG but is drawn up considering the site configuration and functioning of the school.

The basic principle incorporated in this Access Policy and which is the common thread in the development of all access control procedures is:

Only those persons who have been positively identified are allowed to enter the school premises.

This basic principle applies at all times, for all the periods of the year (including holiday periods) and in particular situations, such as (non)-recurrent events.

The following guidelines focus mainly on access management for daily operations. A separate section is dedicated to special events.

4. Scope of application of the Access Policy

This access policy applies to the European School of Mol.

5. Applicable legislation

This Access Policy document describes the minimum standards for the development of access procedures in the schools. If local legislation deviates from the minimum standards developed in this Policy document, the former has precedence. Documented evidence of this deviation must be presented by the school when necessary and upon request.

In Belgium police and law enforcement services do not have right of access to schools' premises, except upon request and by authorization of the School Director.

The processing of all personal data collected and used to guarantee the proper functioning of the access management system must be in accordance with the General Data Protection Regulation (GDPR) and the national privacy laws.

6. Responsibilities and Accountability

According to the General Rules of the European Schools, the Director of the school is responsible for the security on school premises. All security-related access procedures must be approved by the school director.

The School Director is responsible for the central administration of access control measures for the school facility and designates the responsibility of developing procedures to the DDFA and SSO. He/she shall provide advice and recommendations regarding the development and maintenance of access control measures for the respective areas of the school premises, such as:

- developing access security related procedures;
- managing contracted services with respect to all aspects of access control;
- approving the installation, management and maintenance of all access control systems for the schools; and
- approving all requests for access cards and/or keys before being issued.

In the event of an emergency, protection of life and school safety will take precedence over the Access Procedures on the school compound.

[1] Photographs are allowed as long as they are not processed through a specific technical means allowing the unique identification or authentication of a natural person (recital 51 of the GDPR)

7. Description of the different user groups

Our campus has two accesses (main gate and cycle gate behind Primary) allowing persons, vehicles, bicycles, and the like, to enter the school premises. These accesses are properly secured by Securitas in order to avoid intrusion. The main gate is equipped with security barriers, combined with a sticker control access system for cars, visitor access control procedures and security guards.

As mentioned above, and at all times, only persons who have been announced, positively identified with ID upon arrival and license plate can have access to the campus.

Hereunder is a description of the minimum-security requirements applicable to the different user groups accessing the campus. For the ease of understanding and the clarity of this document, six main user groups are identified in this document.

- Category 1: Population present on the school compound on a daily basis, linked to the core business of the school
- Category 2: Pupils
- Category 3: Population present on the school compound on a daily basis, linked to the activity of the school itself (cleaning, maintenance,…), the Parents Association and the day care provider.
- Category 4: All services providers of the Parents Association and the day care provider (busses, canteen, extracurricular activities).
- Category 5: Parents of school and day care.
- Category 6: All others not belonging to category 1 to 5.

Category 1: Population present on the school compound on a daily basis, linked to the core business of the school

- Employees (teachers, staff, administrative and ancillary staff (AAS)
  All staff employed directly by the school, the seconded staff, AAS, irrespective of the type of contract they possess (permanent or temporary).

- Interim workers:
  Every person employed by the school *ad interim*. From the access security perspective, the school considers the interim workers as "employees". Consequently, the school will provide them with an access card valid for the entire duration of their contract.

- Interns:
  From the access security perspective, the school considers them as interim workers.

Category 2: Pupils

- Pupils:
  All children enrolled by the school from kindergarten, primary school and secondary school.

Category 3: Population present on the school premises on daily basis linked to the activity of the school itself (cleaning, maintenance,…), the Parents Association and Day Care

- External service providers contracted by the school.
  Included herein are cleaning and technical maintenance personnel, etc. List is available with the Securitas personnel.

- Parents Association
  All staff members of the Parents Association on the school premises.

- Day Care

Category 4: All services providers of the Parents Association (busses, canteen, extracurricular activities) and the day care

Service providers and contractors of the Parents Association and day care. This group contains all the different activities and services managed by the Parents Association: canteen, bus transportation, bus attendants, extracurricular activities, etc.

Category 5: Parents

- Parents
  The definition of "parents" comprises all the adults who can be considered under the term "close" family of forming the family unit. It includes the biological parents, stepparents, legal guardian, nurse, etc.

Category 6: All others not belonging to category 1 to 5.

This category contains all persons external to the schools and who are visiting the school for a specific reason. Since the school has little or no information about them, it is important to manage their access to the school premises in a very strict way.

It is also important to consider all potential threats posed by intruders seeking access to the school via fallacious means.

- Visitors

Persons external to the school, not belonging to any other category mentioned in this chapter.

- Technical maintenance personnel

They are not present on site on a daily basis, contrary to the technical maintenance service providers described under category 3.

- Deliverers (not including parcel deliveries)
  Transporters delivering goods ordered by the school or other parties active on the school premises.

- Parcel deliverers

8. ID badges and access cards

An ID badge is defined as a badge that serves to identify the person wearing it.
An access card is defined as card with a microchip or magnetic strip containing encoded data that is read by passing the card through or over an electronic device, used to provide access to restricted or secure areas.

All adults present on the school premises must be easily identifiable at all times by wearing an ID badge. This principle applies to all the above-described categories. For parents during drop off and pick up time this will be done by the use of a pedestrian/bicycle badge.

Depending on the category of the user, the layout and content of the ID badge may differ. The ID-badges for category 1, 2, 3, 4 and 5 users must contain at least:

- the surname and first name of the user; and
- photo of the user and the logo of the European Schools

Each school can add extra features (e.g., colour) to make a distinction between different (sub-)categories of users.
Note: in case of high turnover of some specific users of category 3 and 4 an alternative labelling of the ID badge (to be determined by school) can be used instead of the surname and first name.

The visitors badges for category 6 users will contain the logo of the European School, and an individual badge number. This ID badge is reusable.

the school is partially equipped with an access control system. The school will combine both the functions of ID badge and access card in the same card.

For reasons of convenience, the term "access card" will be used in the procedures described hereunder. This term refers to the combination of the functionalities of ID badge and access card. If the term ID badge is used, this refers specifically to this functionality only. In case a school is not equipped with an access control system, the term access badge will always refer to the ID badge.

9. Minimum requirements for the access procedures to the school premises

The schools access procedures are based on the general principles of the European schools and take into consideration the schools own specificities.

The number of entrances and exits to and from the school premises must is reduced to a minimum of

two: The main gate with 24h surveillance and bicycle/pedestrian gate open directly before and after

school under supervision of a security guard.

All entrances and doors are being closed and locked according to a locking plan.

The risk or tailgating (i.e. an unauthorized person follows someone and slips with him/her through the entrance) is mitigated by means of a double barrier at the entrance.

The access security management of the campus is based on the following procedures:

Access procedures for category 1 users
All category 1 users must be unambiguously identifiable at all times when entering the school premises. This is done by visual check of the car sticker by the security guards. Pedestrians and cyclist are observed by security guards.

Access procedures for category 2 users
From a security point of view, the population of pupils is visually easily and clearly identifiable. Therefore, it must be considered as a low security risk.

Intruding "students" of the age of S6 and S7 students, who are not part of the pupil population, may try to infiltrate the school. The access procedures will have to take into account this particular aspect.

The school buildings are equipped with an access control system. The access rights related to these access cards are linked to the school schedule and the authorization to leave the school during the lunch break.

Pupils of the Primary school are only authorized to leave the school accompanied by the parents or legal guardian.
Pupils of the Secondary school receive one of the three types of school cards (badges) based on the agreement between their legal representatives and the school.

RED CARD

Pupils are not allowed to leave the school during school hours. They are in school each day from the beginning to the end of the school day.

YELLOW CARD

Pupils have permission to stay at home in the morning until their first real lesson starts and return home after their last real lesson of that day. They are not allowed to leave the school grounds during lunch break or free lessons immediately before and/or after the lunch break.

GREEN CARD

Pupils have permission to stay at home in the morning until their first real lesson starts and return home after their last real lesson of that day. During teaching hours immediately before and/or after the lunch break pupils may go home if they have no lessons.
This applies specifically to pupils who live in the neighborhood (provided that parents are at home).

The management reserves the right to decide allocation of this card, based on the student's residential address and the request of the parents. If a free period falls between two lessons, the pupil is never allowed to leave the school premises.

In exceptional cases, you can contact the educational advisors to ask permission for your child to leave the school, even with a red card.

In this context it is important to remember that not only the security of the pupils is involved, but also their safety and the school's liability.

<u>Access procedures for category 3 users</u>
External service providers:

The employees of the external service providers that require daily presence at school (cleaning, canteen, PA staff, Day care) are considered, from an access security point of view, as "employees". This implies that they will receive an access card (with predetermined access rights).
Replacements of the regular employees of the external service providers will be considered as visitors and follow the procedures accordingly.

The school has a procedure to detect attempts of fraud by the access control with the car stickers.

Parents Association:
The Parents Association is an organization that is independent from the school, and must consequently be considered as a third party, despite the fact that its members and activities are present throughout the school premises. This being said, it is desirable that the school facilitates access to its premises for the staff members of the Parents Association, whilst maintaining a high level of security. Considering the fact that the school remains at all times responsible for the security on its premises, the access security requirements for the Parents Association cannot be less stringent than those for the school personnel. Every school year the school issues updated access procedure to the PA. This document contains the following elements:

- the procedures to follow for the request and creation of access cards;
- the duration of validity
- procedures in case of loss
- communication procedure to guarantee that all data are up to date;

- To ensure and maintain the required level of security, it is essential that the school remain the issuing authority for all access cards, their activation and deactivation. Under no circumstance should this responsibility be delegated to subordinate or independent bodies;
- the description of the applicable security rules on site;
- the procedure for providing access to persons without access card;
- communication modalities to ensure all data are at all times up to date;
- eventual access rights to the car park;
- access hours;
- access rights;
- …..

The school has the authority to audit the access security procedures of the Parents Association and their service providers. In case of irregularities the Parents Association will have to comply immediately with the corrective measures formulated. If the non-compliance persists, the school can take and/or impose the appropriate measures with respect to the Parents Association. It is reminded that the school is ultimately responsible for the security.

<u>Access procedures for category 4 users</u>
The service providers of the Parents Association and the day care are third parties on the school premises working under the authority of the Parents Association or the day care. Their activities lead to the daily presence of many people on the school premises, potentially creating important security risks if not properly managed.

The Parents Association and the day care are responsible for the security management of their respective service providers. To guarantee a proper security level, the agreement between the Parents Association or the day care and the school, will also contain at least:

- the description of the responsibilities with regard to their service providers;
- the list of service providers allowed to have access cards;
- the description of the applicable security rules on site for the service providers;
- the description of the modalities concerning the possibility to provide access cards, including access rights, accessible areas, access hours, etc.;
- the description on an operational level of the security areas in which the school collaborates with the Parents Association and relevant modalities;
- possible access rights to the car park; and
- communication modalities to ensure that all data are at all times up to date.

Access procedures for category 5 users

- The school allows parents to have access to the school premises.
- Collective access (at the beginning and end of the school day) to the school premises. All parents accessing the school can be identified by means of the Car sticker that is requested at the start of the school year.
- Individual access at any other time of the day. The parent are considered as a category 6 visitor and must register before entering the school site, regardless of the car sticker.

The access procedure of the school contains specific procedures on how to deal with parents who have an access ban to the school premises due to risks such as, but not limited to:

- kidnapping of a child (legal order); and
- aggression of school personnel.

In such a situation the school must inform the Security Guard with the name of the parent and license plate number of the vehicle that is not allowed to enter the school premises anymore.

Access procedures for category 6 users

Requirements for visitors, technical maintenance (not present on site on daily basis as the technical maintenance service providers described under category 3) and delivery personnel. The access is controlled with following guidelines:

- the obligation to register category 6 users prior to their arrival by their host in a visitor announcement system;
- the ID verification of the announced category 6 users upon arrival on the school site;
- the ID verification of category 6 users who have not been announced in the announcement system. The security guard will contact the person concerned by phone to check if the visitor is expected;
- the registration of the visitor and all the data (full name, license plate, host) collected in the visitor's log; and
- the conditions of use for durable ID badge or visitor's access card.
- the obligation for visitors to wait on the main parking until the host picks them up. Exceptions can be made for visitors who are regularly on the premises and know their way around.
- the Communication of the emergency procedures and the designated collection points.

Remark for delivery personnel (not including parcel deliverers)

All sorts of deliveries are to be expected in the school. Usually delivery personnel will arrive in lorries or vans. Ideally each arrival of a delivery should be announced in the visitor announcement system. Practically this is not always feasible. Therefore, the school can decide to additionally implement a procedure to verify, with the department or person concerned by the delivery, if the delivery is expected. Only after positive verification can the delivery personnel enter the premises of the school. During the time of presence on the school premises, the delivery person is supervised at all times. The school must determine the means to put in place in order to meet this goal, (e.g., accompanying the deliverer by the workmen, surveillance by CCTV,…)

Parcel delivery personnel

Parcel deliveries should happen at the school entrance at the guards kiosk or at a fixed designated place in the school. Parcel deliverers should not enter the school premises.

For large parcels (e.g., pallets, very heavy parcels), the procedure for deliverers can be followed.

The school will control the content of the parcel in a safe and separate location (near the garage).

Remark: the delivery of private parcels to the school is strongly discouraged.

Exceptions
Exceptions to the above described requirements can be made for individuals or subgroups of a specific category. If such exceptions are allowed, the school will have to justify the allowed exception (for example, government representatives of the governmental building agency)

10. Minimum requirements for the access of vehicles

Vehicles can pose a serious security threat. The vehicle itself can be used as a weapon (ram raid) or it can be used to bring weaponry or illicit products onto the school premises. On the other hand, the danger of keeping cars outside of our premises causes bigger safety and security threats than allowing them in school. Therefore, it is essential that only vehicles allowed to access the car parks inside the secured perimeter of the school premises, can enter them.

Depending on the user category, the following access requirements apply.

Access procedures for category 1 users
The school grants access to the vehicles of category 1 users. The category 1 user will have to file a request for access to the school premises and will receive a car sticker that gives them access to the school premises.
All vehicles having access to the school premises must be registered in a database with the name of the owner and the license plate number of the car.
The car must be identifiable by a sticker apposed on the wind shield for identification.
For different reasons (for example servicing of the car), it may be that the user arrives with another car. In this case the driver's identity must be verified as well as his access rights to the car park, before providing access to the school premises.

Access procedures for category 2 users (students)
This user category can have access with a vehicle to the school premises. The category 2 user will have to file a request for access to the school premises and will receive a car sticker that gives them access to the school premises.
All vehicles having access to the school premises must be registered in a database with the name of the owner and the license plate number of the car.
The car must be identifiable by a sticker apposed on the wind shield for identification.
For different reasons (for example servicing of the car), it may be that the user arrives with another car. In this case the driver's identity must be verified as well as his access rights to the car park, before providing access to the school premises.

Access procedures for category 3 users
The school can decide to grant access to the vehicles of this user category. The Parents Association and the day care have to file a request to the school management for access to the school premises. In this case the requirements for category 1 users apply.

Access procedures for category 4 users
A distinction must be made between service providers working on site (for example extracurricular activities) and other service providers.

Service providers working on site:
The PA and the day care have to file a request to the security guard for access to the school premises.They follow the access procedures for category 6 visitors.

Service providers on site for a short term (e.g., busses):
These service providers can only have access to the school premises after having received the consent of the school. If the school consents to grant access, the PA and the day care will communicate to the school the list of names and their license plate numbers to the security guards.
Only vehicles on the list will be given access to the school premises.

Access procedures for category 5 users

This user category can have access with a vehicle to the school premises. The category 5 user will have to file a request for access to the school premises and will receive a car sticker that gives them access to the school premises.
All vehicles having access to the school premises must be registered in a database with the name of the owner and the license plate number of the car.
The car must be identifiable by a sticker apposed on the wind shield for identification.
For different reasons (for example servicing of the car), it may be that the user arrives with another car. In this case the driver's identity must be verified as well as his access rights to the car park, before providing access to the school premises.

Access procedures for category 6 users
It is preferable to keep the vehicles of visitors on the main parking of the school premises. All visitors must be registered in the announcement system to have access to the school premises, clear procedures must be implemented containing at least the obligation to communicate their name, license plate, host, date and time of the visit in the visitor announcement system. Upon arrival ID verification is performed by the security guard.
Visitors that are not announced need to be registered in the announcement system and verified with the host before allowing access to the school premises.

Technical maintenance providers, contractors, etc., often need access to the school premises because of the equipment and materials required to perform the work. They will be given access after due ID verification of the persons. The security guard can control the vehicle and its content if necessary.

Delivery personnel often require access to the school premises because of the size and/or weight of delivered materials. They will be given access after due ID verification of the deliverer. The security guard can control the vehicle and its content if necessary.

If the driver does not agree to the check, he/she may not enter the school premises, neither on foot nor by vehicle.

Parcel deliverers must be kept outside the school premises as much as possible. If access is granted, the same regulations apply as for the other delivery personnel.

11. Minimum requirements for access within the school premises

The access procedures for entry into the school differs from access control within the school premises. Only authorized persons can access rooms and classrooms by means of an access badge with possibility to limit the classrooms that are accessible as well as a limit in time of 1 week.

Here are a few examples of security and safety risks on the school premises:

- Security risks: theft, access to important documents, access to server room, access to classrooms, etc.
- Safety risks: access to laboratories, access to technical rooms/shafts, roofs, storage rooms, cleaning products, etc.

The school manages access to all these rooms on the school compound in such way that only authorized persons can have access to these with their personal badge.

The school has a clear overview of the access rights linked to access cards to guarantee a secure management of the access rights of the different persons present on the school premises.

The use of an electronic key system is an important part of the security access procedures on the school compound and is properly designed and managed, since they provide any individual with access to restricted areas. The key system policy, is a balance between the security requirements, on the one hand, and the needs of the individual on the other. Every

The school's key system is designed in such a way that it provides a secure and easily-controlled, manageable system.

12. Access card management procedures for long-term access cards

Preliminary note:

This section, and the following one, contain the terms "long term" and "short term". The use of each of these terms is not related to an exact definition of time. To interpret these terms correctly, both the duration of validity of the access card and the type of activity must be considered. In most cases the use of both terms is obvious. For example, an employee of the school will receive a long term access card, a person visiting the school for one day or a couple of hours will receive a short term access card.

For some activities this is less obvious and the school will have to make motivated choices. Activities can, for example, last for an extended period of time and still be considered as "short term" in terms of access security. One such example is a contractor realising construction works on the school premises during 2 months. Although the duration of the works can be considered as "long term", the fact that the school is working with a contractor not linked to the school will result in classifying this as "short term" in terms of access security.

The following procedures are implemented.

12.1. Access card request and issuing procedure

The procedure for the creation and issuance of an access card is determined prior to its implementation and is accessible to all actors in the process. Such procedure should be subject to a review by the school's Data Protection Officer (DPO) before issuance, to ensure GDPR and national privacy laws compliance.

The procedure must contain at least the following elements:

- The description of the administrative procedure for introducing a request for an access card, including the template of the form used for the request;
- The description of the processing of the request including at least the determination of the duration of validity of the access card and the allocated access rights;
- The description for the approval of the request by the Director or his/her designate;
- The process for issuing and activating the access card, including the description of the issuing department;
- The description of the delivery process of the card, including at least proof of receipt of the access card and the user guidelines by the user.

12.2. Duration of validity of access cards

12.2.1. Standard duration of validity

- In case of a request for an indefinite period of time, the duration of validity of the access card is limited to 7 days after activation. After this period, the duration of validity can be extended for another 7 days by updating the badge on site.
- In case of a request for a definite period of time, the duration of validity of the access card must be limited to the expected period of time.
- Exception for example an interim worker with contracts which are renewed on a weekly basis can have an access card with a duration of validity closer to the expected duration of the interim job.)

12.2.2. Procedure at the end of the contract of an access card holder

- The access card must be deactivated at the end of the last workday of the person.
- The access card holder must return the access card to the school at the end of his contract when returning the ICT equipment or at the end of validity at the latest. The access cards remain school's property at all times. A handover document will be signed by both parties.
- At the latest, one month after the departure of the person, all personal data and its user history is deleted. In case of suspicion of fraud, the data can be stored for a longer period with the written authorization of the school Director or his/her designate.

12.3. Access rights:

- As a general principle, the access rights granted by the school are limited. Users are given access only to predetermined areas. The application of this principle will mitigate a number of safety and security risks on school premises.
- The school has defined a set of predetermined user profiles. A specific user will then be linked to a specific user profile.
- The user profiles take at least into account:
  - The time period of the day during which the access card is active;

  - ○ The weekday (for example working day, weekend,…) during which the access card is active;
  - ○ The periods of the year during which the access card is active;
  - ○ The accessible areas of the school, if the same access control management system is used inside the school as for the perimeter.
- Special attention is given to the access rights of certain sensitive areas, for example the server room, laboratories, etc. Only authorized staff members will have access.
- Allocating specific access rights for an individual can exceptionally be accepted. In this case this choice must be motivated.

12.4. Particular situations

12.4.1. Procedure in case an access card is lost, stolen or damaged

The school has:

- an internal procedure to deactivate the badge immediately after the loss of the card is reported; and
- the procedure for the request to replace the deactivated access card.
- The lost, stolen or damaged card is deactivated and cannot be used ever again.

12.4.2. Procedure in case of forgotten badge

A person forgetting his/her badge is a situation that can happen from time to time. Mostly, this is a no or very low risk situation. Nevertheless, an ill-intended person (for example, member of personnel released under unfavourable conditions) may seek to enter the school in this way. Therefore, each person presenting him/herself without access card will have their identity checked, including verification with the school management or the designated replacement.

12.5. User guidelines :

The schools has user guidelines for all persons with a long term access card. These contain:

- The access card shall at all times be clearly displayed by all persons inside school premises.
- It is strongly recommended not to wear the access card in a visible way outside the school premises.
- The access card is strictly personal.
- The measures taken in case of user fraud with an access card.
- The procedure to return the access card to the school, at the expiry date of the access card or at the end of the contract of the card holder.
- The obligation immediately to report the loss or theft of the access card. The school provides the contact details (mail/phone) for reporting of loss or theft via the ICT request form.
- The procedure to follow in case of loss of the access card.
- The access card remains the property of the school at all times.

13. Access card management procedures for short term type access cards

The following procedures is implemented.

- The duration of validity of the access card will not exceed the duration of the stay on the school premises.
- All persons accessing the school premises qualifying for a short term access card, must be registered prior to their visit in the visitor announcement system. If they are not registered, the security guards will have to control whether they were expected by the school. If not, access to the school premises will be refused.
- Procedure for the security guards:
  - o ID verification (note: not all countries allow security guards to ask for the ID card/passport of persons. Alternatives include asking for a driver's license)
  - o Registration in the visitor's log. The visitor's log will contain at least the following information:
    - ▪ Surname and name of person
    - ▪ Name of host
    - ▪ Organization
    - ▪ Time of arrival
    - ▪ Time of departure
    - ▪ License plate number (if applicable)

- The person will receive a visitor's access card before entering the campus. The access card shall at all times be clearly displayed during the entire stay on the school premises.
- The visitor's access card is reusable.
- Reusable visitor's access cards must be returned to the school when leaving the school premises.

Visitors for the Parents association and day care working on the school premises will register their visitors following the same procedure as the school.

14. Access control system

The school's DPO is involved to ensure that the access control system is GDPR compliant as well as the contract to be executed with the supplier.

The access control system for cars is used to secure the accesses of the outside perimeter, the key card system

is used for on site security. The access control system meets the following technical minimum criteria:

- The access control system is a centralized access system.
- The management system of the access control system is password-protected and passwords are regularly changed.
- In the future if technologically possible, the fire, intrusion and CCTV system will be linked to the access control system. As such an integrated security management system can be set up.
- Only the persons appointed by the Director or his/her designate, have "administrator" rights to the access control system.
- Other user profiles (SSO, HR, guards,…) with specific access rights can be created. The access rights linked to a specific user profile is approved by the Director or his/her designate. For each user profile the accessible data and possible operations, must be limited to the minimum requirements necessary to do their job.

15. Intervention procedures

The school develops and implements intervention procedures to deal with the following situations:

- Attempt to enter the school premises in an unauthorized manner;
- The discovery of the presence of an unauthorized person on the school premises;
- A person posing a security threat inside the school premises;
- Attempt of a pupil to leave the school in an unauthorized manner;

16. Reporting

The school implements a reporting tool for security incidents. Two types of reporting are distinguished:

Daily reporting:
The security guards communicate a daily activity report to the Director or his/her designate. This report must contain, besides the overview of the daily activities, the description of all access security incidents.

Trimestral and yearly reporting is done by Security company:
On trimestral and yearly basis, a statistical report of all incidents that have occurred per type of incident. The analysis of these data will allow the school to continuously improve the existing access procedures.

A retention period is foreseen for the reports containing personal data. The School's DPO must be involved to ensure compliance with data protection requirements.

17. Technical maintenance of the Access control system

A maintenance contract will be concluded with a qualified service provider for the maintenance of the access control system. Maintenance of both infrastructure and software must be included.

18. Data protection

The school’s DPO is involved in the elaboration of the access card management procedure and the security guards procedure to ensure GDPR and national privacy laws compliance.

The school’s DPO is in charge of drafting the respective(s) Privacy Statement(s), following the usual structure of the other European Schools’ privacy statements, including:

- Categories of personal data collected;
- Purposes for which personal data are collected;
- Legal basis for the processing of personal data;
- Access and sharing of the collected personal data;
- Protection and security of the personal data;
- Retention periods;
- Data subjects’ rights; and
- Who to contact in case of a complaint.

Data processing activities are recorded in the Register of Processing Activities available on the DPO Portal.

19. Cybersecurity

The Access Control System used should be equipped and reinforced with an adequate IT and cyber security solution. Due to the sensitive nature of the information stored in and managed by the system, a proper cybersecurity protection is necessary. One of the main goals of cybersecurity defense is information protection. Information protection is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide integrity, confidentiality and availability.

The Access Control System/solution provider should ideally be ISO certified according the ISO/IEC 27000/27001 standards (https://www.iso.org/isoiec-27001-information-security.html).

Hereunder is a non-exclusive list of essential cybersecurity controls required for reinforcing the cybersecurity of the access management solution:

- Risk management : IT risk management related to the Access Control System should be performed on a regular basis.
- Identity and Access Management (IAM) – strict access control to the system

IAM security is an essential part of overall IT security that manages digital identities and user access to data, systems, and resources within the application. IAM security includes the policies and technologies that reduce identity-related access risks.

- Update and patch management : The Access Control System software as well as the system environment should be regularly patched and updated. Patch management is an absolutely essential element of the cybersecurity vulnerability and patching strategy. A patching strategy should include reviewing of security patches released, selection & prioritizing of required patches as well as testing patch compatibilities.
- Perimeter security : Perimeter defence of both the physical perimeter as well as the network perimeter security are an essential and indispensable part of cybersecurity defence.
- Monitoring and supervising : IT monitoring comprises a broad class of solutions designed to analyse and determine whether IT equipment is online and performing to expected service levels, while resolving any detected problems. IT monitoring solutions are required for granular examination of the system performance, and automatic alert when problems are suspected.
- Incident management : An incident management process is a set of procedures and actions taken to respond to and resolve critical incidents - how incidents are detected and communicated, who is responsible, what tools are used, and what steps are taken to resolve the incident.
- User and power user training : End user training as well as power user training are an essential component of cybersecurity defence. Training of users is necessary to avoid security risks caused by human errors.
- Business continuity and proper backup solution : Business continuity is the processes, procedures and activities needed to ensure that an organization can continue to function through an operational interruption. This should comprise the necessary procedures and routines for the eventual unavailability of the Access management system. Another essential part is the routines and procedures for disaster recovery, for restoring the system functionality and availability. An indispensable condition for disaster recovery is a proper backup solution accompanied by appropriate backup routines.

20. Events

Events comprise all sorts of activities that lead to an aggregation of people on the school premises.
The definition of events comprises: parents meetings, cultural events, university fairs, profession and orientations days, meetings, graduation ceremonies,…

Events introduce particular security risks linked to the presence of potentially large groups of people, who usually arrive in a short period of time. Combining the management of handling a large number of people, with maintaining a high security level is challenging. This notwithstanding, all persons accessing the school premises during school hours must be positively identified.

This goal is obtained in several ways: individual ID verification of the persons entering the school premises (small scale events); by the use of a visitors list or by the use of a QR code sent to the attendees allowing to control all persons entering the campus.

21. Alert levels

Terrorist threats have become a common element of which we must take account as we manage public institutions and services. The European Schools, being closely linked to the EU Institutions, as compared to ordinary schools, could therefore be more vulnerable to terrorist threats.
To mitigate the risk of a terrorist attack, a system of alert levels has been developed. The four levels of alert are defined as white, yellow, orange and red, whereby white is the lowest and red the highest alert level.

The alert level in which the school operates is determined by the host country's alert level or by the European Commission. The highest alert level will prevail.

The four alert levels are defined as follow:

White: normal operations
Yellow: increased vigilance due to a threat which is unlikely to happen
Orange: increased vigilance due to a threat which is likely to happen

Red: imminent threat

The higher the alert level, the more stringent the access control measures become and the less people will have access to the school premises.

All changes in alert level will be communicated to all persons working on the school premises. The school will determine the most appropriate way to communicate this information. Elements for consideration in the communication are:

- order of priority for different departments, functions and persons to receive the information;
- content of the information (need to know principle) communicated to each department, function and person; and
- possible emotional (over)reaction from persons.

The following security measures apply for each alert level.

White level

The normal operating procedures for the school apply. No additional restrictions are imposed.

Yellow level

The additional security measures to put in place, in addition to the previous level include:

- Only the entrances essential for the functioning of the school will be used. All others will be locked.
- A security guard must be posted at every entrance in use.
- Security guards can perform random security checks of luggage and vehicles entering the school premises.
- Visitors do not have access to the school car park, unless explicit authorisation by the Director or his/her designate.
- Visitors must be accompanied by a staff member during their entire stay on the school premises.
- Larger events can be organized only following a security assessment by the SSO.
- The guard's kiosk must be permanently manned.

Orange level

The additional security measures to put in place, in addition to the two previous levels include:

- Reduction of the school opening hours to the minimum required to guarantee the school's operations;
- Car parks are closed for all vehicles except for vehicles of school staff;
- Events and non-urgent meetings on site are postponed;
- Visitors do not have access to school premises.

Red level

The additional security measures to put in place, in addition to the three previous levels include:

- Staff will receive specific instructions;
- School activities are reduced to a minimum;
- Learning at distance is prioritised;
- Car parks are closed for all cars;
- Most staff is to leave the premises;
- Telework is prioritised;
- Field trips are cancelled.

22. Review clause

A revision of this document is carried out biennially by the OSG.

It is revised by the Safety & Security Officer (SSO) of the OSG, including at the request of any European School of MoI following experience in implementation; or in the case of exceptional circumstances that may compromise or lead to a modification of the guidelines outlined in this document.

The directors, the SSO's of the European Schools and the OSG, may make proposals for revisions at any time. All proposals for revision are to be transferred by email to the SSO of the OSG.

The SSO of the OSG will prepare a list of revision proposals. This list will be submitted to the Secretary General and the directors for examination and approval. The Access Policy Document will then be amended accordingly and a finalised draft will be submitted to the directors of the schools for final approval.