



Kontoret efter stängning: vem har tillträde?

När arbetsdagen är slut förändras kontorets riskbild. Färre personer är på plats, vissa rum ska vara begränsade och en gammal behörighet kan vara svårare att upptäcka än en uppbruten dörr.

PUBLICERAD	12 september 2026
FÖRFATTARE	Siren Techs ingenjörsteam
LÄSTID	6 min läsning

Riskscenario: en behörighet lever kvar

Tänk er att en konsult avslutar sitt uppdrag men att ett passerkort eller en digital behörighet inte spärras i samma takt som övriga konton. En passage sker efter ordinarie arbetstid. Dörrsystemet registrerar händelsen, men mottagare och uppföljning är inte definierade.

Scenariot beskriver en möjlig svaghet, inte en specifik kundincident. Det visar varför fysisk access, roller och rutiner för avslut behöver följas som ett sammanhängande flöde.

Börja med roller och zoner

Huvudentré, personalingång, serverrum, förråd och garage har olika behov. För varje zon behöver verksamheten bestämma vem som får gå in, under vilka tider och vem som granskar en avvikande passage.

Arbetsmiljöverket lyfter att ansvar, riskkartläggning, kända rutiner och regelbunden uppföljning behöver hänga ihop. Tekniken bör stödja det arbetssättet i stället för att ersätta det.

Kontroller som minskar osäkerheten

Kontrollera behörighetsflödet med samma noggrannhet som själva dörren.

- Finns en ansvarig för att lägga till, ändra och spärra användare?
- Är behörigheter avgränsade efter roll, dörr och tid?
- Kan en avvikande passage kopplas till rätt mottagare och uppföljning?



- Testas rutinen när någon byter roll eller lämnar verksamheten?

Så kan Siren System bidra

En konfigurerad accesslösning kan hantera användare, styra åtkomst efter roll och tid och visa passageloggar i Siren Portal. Kameror, sensorer och incidenthantering kan ingå när de behövs för den valda kontorslösningen.

Lås, kort och befintlig teknik måste kontrolleras innan kompatibilitet bekräftas. Alla kontor behöver inte samma produkter eller samma behörighetsmodell.

Vad lösningen inte gör åt er

Systemet avgör inte vem som ska ha tillträde och ersätter inte rutinen för onboarding, rollbyte och avslut. Det garanterar inte heller att varje incident förhindras.

En kostnadsfri säkerhetskonsultation kan användas för att gå igenom entréer, begränsade rum, befintlig teknik och ansvar innan produkter och funktioner väljs.

Källor och vidare läsning

[Boka demo för kontorssäkerhet](#)

[Se lösningen för kontorssäkerhet](#)

[Arbetsmiljöverket: arbeta systematiskt med risker](#)



The office after closing: who has access?

When the working day ends, the office risk profile changes. Fewer people are present, some rooms should be restricted and an outdated permission can be harder to detect than a forced door.

PUBLISHED	12 September 2026
AUTHOR	Siren Tech's engineering team
READING TIME	6 min read

Risk scenario: a permission remains active

Imagine that a consultant finishes an assignment but an access card or digital permission is not disabled at the same pace as other accounts. A passage occurs outside normal working hours. The door system records the event, but the recipient and follow-up are not defined.

The scenario describes a possible weakness, not a specific customer incident. It shows why physical access, roles and offboarding procedures need to be followed as a connected workflow.

Start with roles and zones

The main entrance, staff entrance, server room, storage and garage have different needs. For each zone, the organisation needs to decide who may enter, at what times and who reviews an unusual passage.

The Swedish Work Environment Authority stresses that responsibility, risk assessment, known procedures and regular follow-up need to work together. Technology should support that way of working rather than replace it.

Controls that reduce uncertainty

Review the permission workflow with the same care as the door itself.

- Is someone responsible for adding, changing and disabling users?
- Are permissions limited by role, door and time?



- Can an unusual passage be connected to the right recipient and follow-up?
- Is the procedure tested when someone changes role or leaves the organisation?

How Siren System can contribute

A configured access solution can manage users, control access by role and time and show passage logs in Siren Portal. Cameras, sensors and incident handling can be included where needed for the selected office solution.

Locks, cards and existing technology must be checked before compatibility is confirmed. Not every office needs the same products or permission model.

What the solution does not do for you

The system does not decide who should have access and does not replace procedures for onboarding, role changes and offboarding. Nor does it guarantee that every incident will be prevented.

A free security consultation can be used to review entrances, restricted rooms, existing technology and responsibilities before products and functions are selected.

Sources and further reading

[Book an office security demo](#)

[See the office security solution](#)

[Swedish Work Environment Authority: systematic risk prevention](#)