



Smart Working and Security

Smart Working is an approach that embraces new technological possibilities to be always operational at any location. It also acknowledges current trends in society like the disappearance of barriers between the private and professional lives of employees. It focuses on output rather than input, with the emphasis less on how you get the results and more on the results themselves. It is fundamentally a different employment experience that company? How do you make sure that the new working environment maintains the same security level? Do you need to adjust your security policy? How can you support smart working without taking irresponsible security risks towards your organization and employees?

An introduction to 'Smart Working'

IT companies have been working for years on making electronic devices available to anyone, at any moment and at any location. Today's smart phones, laptops and tablet PCs allow people to be productive and do their work at all kinds of places and times. The modern professional doesn't want to be dependent on a fixed working space with a computer. He wants to have access to information and applications readily available, for example while traveling by train or while waiting at the airport.

Architects, interior designers and facility managers have also noticed this trend and observed righteously that the traditional office building doesn't support and stimulate

this new way of working. That's why more companies decide to choose modern office design based on the flexible use of workspaces and the optimal facilitation of communicational and inspirational aspects within the office buildings.

What does this have to do with security?

'Smart Working' is strongly related to security. Employees are more mobile than ever before and they expect their employer to provide the means to make them productive at any location, inside or outside the office. How do you secure these employees and the business assets they carry with them, without hindering them?

Your office will turn more and more into a meeting place and workspace for those activities that cannot take place in a virtual environment. What impact does this have on your access control policy? How do you take care of enough security in an organization with an increasing number of semi-public zones in which a wide variety of people execute all kind of activities?

In principle, people no longer have fixed workspaces; they are supposed to empty their temporary desk if they are going somewhere else for a longer period of time (for a meeting, for example). Where can they leave there belongings in a smart and safe way? A personal locker might be the obvious answer. But how can these, sometimes large numbers of lockers, be easily managed?

Conflicting interests?

'Smart working' gives people responsibility instead of boundaries. It encourages them to take the initiative and develop entrepreneurship within the organization. Security measures, however, are often restrictive. Don't these interests conflict with one another?

At first sight, it may not look easy for a security manager to accept and support the principles of 'Smart Working'. But it's definitely possible to implement 'Smart Working' without making any concessions to your security objectives. For all that, it's important to keep a few things in mind.



A new way of working implies change. Changes to reach that new way of working, but also changes to maintain that new way of working. Your access control and security management system has to be capable of handling these changes. Configurations and settings must be flexible. Furthermore, your system must offer the possibility to change the security level with one push of the button. The functionality of AEOS is based on software and can be configured easily, in order to deal with these changes.

Locker management

If people don't have a fixed workspace, they are often asked to clean their flexible workspace if they don't use it for more than half an hour. This means that people use more than one workspace per day, possibly even spread over several locations. In these cases, people want to have the possibility to store their personal belongings temporarily. This can be solved easily by placing lockers with an electronic locking system from Nedap at strategic places in the organization. This makes sure that desks are clean at the end of the day, but also that the risk of information being spread unwittingly is reduced considerably. The lockers use locks with integrated card readers and can be combined with the AEOS access control system. One of the advantages of this is that people can use their access badge to get access to a locker as well. Another advantage is that the lockers can be managed from the access control system, so you only need one system for security and locker management. All functionalities of AEOS, like the use of groups, time schedules and a log book, can be applied to lockers as well. Thus, from one integrated system, the access to the building and the use of lockers can be managed and controlled.

Dynamic locker allocation

The AEOS and LoXS integration can also be used for the dynamic allocation of lockers. This means that instead of having access rights for one fixed locker, people can claim any available locker. This can be convenient in areas with more potential users than the number of available lockers. The dynamic locker functionality makes locker management more efficient and flexible and is ideal for flex work environments.

A proper management system will support the concept of roaming users and enables centralized administration of lockers across an estate of multiple, possibly wide spread buildings.

Access control at micro level

If you want the access to documents and other valuable and important assets to be regulated in a well managed way, you can consider implementing access control at your cabinets. This is what we call 'micro level access control'. By applying the principles of AEOS access control on cabinets, you can manage the cabinet doors just like the normal doors in your organization. This way,

valuable assets, such as multimedia projectors, bank cards and personnel files, can be safely stored. At the same time, the scope of the company's security policy is expanded. And the good thing is that integration with systems for intrusion detection and camera observations stays intact.



Physical and logical access

The paragraph above about micro level access control illustrates that integration of systems is important. This is also the case for physical and logical security; they should no longer be seen as separate pillars. If access to data files and buildings is based on the same policy and the same principles, a company's overall security can be greatly improved. The connection between Imprivata OneSign and Nedap AEOS provides a good solution to bridge the gap between AEOS events and IT network access. This physical/logical connection maps identities contained within the access control system and IT directories, making it possible that people can only log on to the system if they have received access to a physical location by presenting an authorized badge.

'Smart working' is about using the individual and joint strength of your employees. That's why these employees should be hindered as little as possible by security measures and be supported as much as possible. Therefore, the daily use of the security system must be quick, intuitive and hassle free. Whether you use an

access badge or biometrics the goal is to give users access to spaces, cabinets, lockers, printers and other systems, with only one means of identification. This is possible with modern tools and devices.

'Smart working' is not a threat for the security or for the security manager. It's the ultimate chance to show your organization that security is more than restrictive policies and complicated systems. Introducing these new ways of working is the perfect opportunity to spice up your security and to demonstrate that security and empowerment of employees really can go hand in hand.

