



SECURITY DICTIONARY

SDS is pleased to offer you its short security glossary to share the significance of mastering these particular words in this domain.

Mastering language is intellectualizing ideas. In security, various ideas lead to a concept. This concept allows for designing genuine security suited to real needs instead of imaginary fears.



SDS มีความยินดีที่จะเสนออภิธานศัพท์ด้านความปลอดภัยซึ่งจะช่วยให้คุณเข้าใจถึงความสำคัญของการเรียนรู้คำศัพท์เฉพาะเหล่านี้

การเรียนรู้ภาษานี้หมายถึงการทำให้ความคิดของคุณเป็นจริงและออกแบบการรักษาความปลอดภัยที่แท้จริงซึ่งเหมาะสมกับความต้องการที่แท้จริงแทนที่จะรู้สึกหวาดกลัว

EXPERTISE

Expertise (consultancy, audit, evaluation, advisory) is the upstream study for all the possibilities to implement the best security at the best price.



ความเสี่ยง

ความเสี่ยงแสดงถึงความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้นโดยที่มนุษย์ไม่สามารถควบคุมได้ ความเสี่ยงนี้เป็นที่ทราบกันทั่วไป คาดการณ์ได้ และหลีกเลี่ยงไม่ได้ และปัจจัยที่ไม่ทราบเพียงอย่างเดียวยังคงอยู่ในขณะนี้

The risk

The risk represents the possibility that an event occurs without the human being able to control it. This risk is generally known, predictable and unavoidable. The only missing factor remains the moment.

การประเมินความเสี่ยง

การประเมินความเสี่ยงมีวัตถุประสงค์เพื่อหาปริมาณวิธีการปรับใช้เพื่อลดผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์นี้ให้ได้มากที่สุด

Risk assessment

The risk assessment aims to quantify the means to deploy in the hope of reducing the potential consequences of this said event as much as possible.

ภัยคุกคาม

ภัยคุกคามคือการตระหนักถึงความเสี่ยงที่ใกล้เข้ามาหรือประมาณการในระยะสั้นมากหรือน้อย

Threat

The threat is the realization of a risk approaching or estimated to occur shortly.

การประเมินภัยคุกคาม

การประเมินภัยคุกคามมุ่งเน้นไปที่การกำหนดกลยุทธ์ในแง่ของวิธีการและมนุษย์เพื่อตอบสนองอย่างเหมาะสมต่อเหตุการณ์ที่มนุษย์สามารถจัดการได้

Threat evaluation

Threat evaluation focuses on establishing a strategy in terms of means and man to respond appropriately to an event or part of, which humans can manage.

ช็อก

ช็อกคือผลกระทบของเหตุการณ์ที่เกิดขึ้นแรงกระแทกส่งผลกระทบต่อมนุษย์และสินค้า

Shock

Shock is the impact from the beginning of the event to the return to normal. The shock impacts humans and goods.

การจัดการช็อก

เป็นวิธีการจัดการช็อกด้วยการตรวจสอบย้อนกลับในระหว่างเหตุการณ์หากเป็นไปได้ในลักษณะของสมุद्रายงาน

Shock dealing

It is the manner the shock is managed. The quality of means, knowledge, and reactivity will significantly affect the way to deal.

วิกฤติ

วิกฤติไม่ใช่เรื่องสำคัญและเป็นผลมาจากภาวะช็อกที่จัดการไม่ดี วิกฤติส่งผลกระทบต่อการเงินและภาพลักษณ์

Crisis

A crisis is the consequence of an inappropriately managed shock.

A crisis is not physical but impacts finances and image.

การจัดการวิกฤติ:

วิกฤติการณ์ส่วนใหญ่เกิดจากการสื่อสารโดยอาศัยข้อมูล มีสามทำให้เลือกในตอนเริ่มต้นและทำต่อไป: ทำรับ ทำขนาน และทำปฏิเสธ

Crisis management:

Most crises are based on the communication of information for conducting according to three postures: acceptance, parallel, and denial. Executives manage crisis management.

การตรวจสอบการปฏิบัติตาม:

เป็นการตรวจสอบความสอดคล้องของการติดตามผลมาตรฐานการปฏิบัติงาน (SOP)

A compliance audit:

It is the conformity check of standard operating procedures (SOP) from your chain, franchise or own internal rule, if any.

ขั้นตอนการทำงานมาตรฐาน:

เป็นข้อบังคับภายในเว็บไซต์ที่ทุกคนจะต้องเคารพ

Standard Operation Procedure:

It is the in-force regulation within the site to be respected by everyone.

การวางแผนการรักษาความปลอดภัย:

ความจำเป็นโดยรวมสำหรับมาตรการรักษาความปลอดภัยที่จะดำเนินการ แยกส่วนและจัดประเภททางการเงินตามลำดับความสำคัญ

Security planning:

It is the estimated overall security measures to take and needs, prioritized, sectorized and financially classified to be budgeted.

การตรวจสอบความปลอดภัย:

กลุ่มการตรวจสอบความปลอดภัยต้องการทั้งหมด เช่น การประเมินความเสี่ยง การประเมินภัยคุกคาม การตรวจสอบการปฏิบัติตามข้อกำหนด การวางแผนความปลอดภัย และกฎความปลอดภัยภายใน

Security audit:

The security audit groups all needs, such as risk assessment, threat evaluation, compliance audit, security planning and internal security rules. It is a factual report with all the potential answers.

BUILDING

We call "building or structure" the overall site property. Security must base on this construction to organize technological and human deployment to secure the site in synergy.



วิกฤติ

วิกฤติไม่ใช่เรื่องสำคัญและเป็นผลมาจากภาวะซ็อกที่จัดการไม่ได้ วิกฤติส่งผลกระทบต่อการเงินและภาพลักษณ์

The surrounding

It is an imaginary area around the property containing all that could impact the site.

การจัดการวิกฤติ:

วิกฤติการณ์ส่วนใหญ่เกิดจากการสื่อสารโดยอาศัยข้อมูล

The periphery:

It is the physical limits of a site.

การตรวจสอบการปฏิบัติตาม:

เป็นการตรวจสอบความสอดคล้องของการติดตามผลมาตรฐานการปฏิบัติงาน (SOP)

Primary access:

It is all various accesses permitting to enter from the surrounding into the site through the perimeter. Primary or direct access should always remain under human control.

ขั้นตอนการทำงานมาตรฐาน:

เป็นข้อบังคับภายในเว็บไซต์ที่ทุกคนจะต้องเคารพ

Sectors:

IA site is usually split into various sectors based on building. The splitting strategy can be to preserve the smooth flow, occupancy, confidentiality or any choice according to the activity.

การวางแผนการรักษาความ

ปลอดภัย:

ความจำเป็นโดยรวมสำหรับมาตรการรักษาความปลอดภัยที่จะดำเนินการ แยกส่วนและจัดประเภททางการเงินตามลำดับความสำคัญ

Secondary access:

It is all accesses within a site that permit to enter from one sector to another. Secondary accesses can be under technological control, depending on the security level.

TECHNOLOGY

The technology is all the systems installed to organize, manage and reinforce the building and support the security officers in their protection mission and detection.



วิกฤติ

วิกฤติไม่ใช่เรื่องสำคัญและเป็นผลมาจากภาวะซ็อกที่จัดการไม่ดี วิกฤตส่งผลกระทบต่อการเงินและภาพลักษณ์

Detection

CCTV, IoT, radars, X-ray, IR and all these devices permit information collection and alert humans for analysis. However, some items like CCTV and IoT are increasingly "intelligent" and can take basic programmed actions under humans' control.

การควบคุม

• การอนุญาตให้เข้าถึง

การอนุญาต" อนุญาตให้คุณเข้าถึง, การอ่าน, การใช้, การปรับเปลี่ยน หรือ ลบข้อมูล เพิ่มข้อมูล หรือสนับสนุน .การอนุญาตให้เข้าถึงข้อมูลอย่างเช่น บุคคล เราเรียกว่า "มีสิทธิ์ที่จะได้รับรู้เรื่องนี้"

• สิทธิการเข้าถึง

สิทธิการเข้าถึง คือ การเข้าถึงเครือข่าย ในพื้นที่ และ การติดตามใช้ข้อมูลที่เข้มงวด , ภายใต้ข้อบังคับของ SOP ,ความเป็นไปได้ในการเข้าถึง ข้อมูลทางกายภาพ,สำนักงาน,พื้นที่ ,หรือขอบเขต , รวมแม้กระทั่งบางเมือง

Control:

• Access authorizations:

The "authorization" allows you to access, read, take, modify or delete documents or supports. Access authorization to the documents is linked to the person. We call it the "right to know about".

• Access right:

The access right is strictly linked to the zone and follows, under the SOP in force, the possibilities to access an area physically, an office, a space or a zone, or even a country ...

การตรวจสอบการปฏิบัติตาม:

เป็นการตรวจสอบความสอดคล้องของการติดตามผลมาตรฐานการปฏิบัติงาน (SOP)

Access control:

The access control is an automatic protocol to allow an ID holder to open access or to be authorised by the operational security to access.

ขั้นตอนการทำงานมาตรฐาน:

เป็นข้อบังคับภายในเว็บไซต์ที่ทุกคนจะต้อง
เคารพ

Identifications (ID):

The ID is the unique sign that identifies its holder and initiates an access chain. The ID can be physical as a Mifare or RFID card, and organic, like fingerprint, voice, face and probably the eye in the future.

การวางแผนการรักษาความ

ปลอดภัย:

ความจำเป็นโดยรวมสำหรับมาตรการรักษาความปลอดภัยที่จะดำเนินการ แยกส่วนและจัดประเภททางการเงินตามลำดับความสำคัญ

Alarm:

It is the signal triggered by an unauthorized or expected action. It can only be a count to be recorded, or it can be relayed.

ขั้นตอนการทำงานมาตรฐาน:

เป็นข้อบังคับภายในเว็บไซต์ที่ทุกคนจะต้อง
เคารพ

Protocol:

A protocol is always associated with an alarm. The protocol indicates the actions to follow in case of triggering.

การวางแผนการรักษาความ

ปลอดภัย:

ความจำเป็นโดยรวมสำหรับมาตรการรักษาความปลอดภัยที่จะดำเนินการ แยกส่วนและจัดประเภททางการเงินตามลำดับความสำคัญ

Closed circuit:

Usually installed in SMEs, all necessary security items and devices are split into various installations that multiply the systems between cameras, access control, and alarms...

ขั้นตอนการทำงานมาตรฐาน:

เป็นข้อบังคับภายในเว็บไซต์ที่ทุกคนจะต้อง
เคารพ

Centralized machine:

This management system permits joining all security devices in one or more physical or virtual servers to be administered in total synergy. This installation gives much more flexibility and possibility than a closed circuit.

SECURITY OFFICERS

Militaries warrant the peace under the Constitution.
Police implement the region's law under justice.
Security Officers warrant the respect of S.O.P.



ขั้นตอนการทำงานมาตรฐาน:

เป็นข้อบังคับภายในเว็บไซต์ที่ทุกคนจะต้อง
เคารพ

The missions

Defined in the SOP, the missions or tasks give the security officer the acts to be taken, the limits of their actions, and the behaviour to be respected.

การวางแผนการรักษาความ

ปลอดภัย:

ความจำเป็นโดยรวมสำหรับมาตรการรักษาความปลอดภัยที่จะดำเนินการ แยกส่วน และจัดประเภททางการเงินตามลำดับความสำคัญ

The reporting:

Reporting unexpected events permits keeping traceability in case of investigations or crises. Crisis management is mainly based on information and reporting.

ขั้นตอนการทำงานมาตรฐาน:

เป็นข้อบังคับภายในเว็บไซต์ที่ทุกคนจะต้อง
เคารพ

The hierarchy:

The employment hierarchy establishes the SOP and the tasks for the guards. The organic hierarchy administrates the guard throughout its career.

การวางแผนการรักษาความ

ปลอดภัย:

ความจำเป็นโดยรวมสำหรับมาตรการรักษาความปลอดภัยที่จะดำเนินการ แยกส่วน และจัดประเภททางการเงินตามลำดับความสำคัญ

The statute:

A guard is a daily worker and cannot work more than 12 hours daily. The guard cannot work for two companies at the same time. He needs to learn at the police academy to be graduated as a security officer.

ขั้นตอนการทำงานมาตรฐาน:

เป็นข้อบังคับภายในเว็บไซต์ที่ทุกคนจะต้อง
เคารพ

The salary:

A guard gets paid monthly for all employed days on the 1st of each month. If the guard does not work for sickness, he is paid on 8 hours based.

การวางแผนการรักษาความ

ปลอดภัย:

ความจำเป็นโดยรวมสำหรับมาตรการรักษาความปลอดภัยที่จะดำเนินการ แยกส่วน และจัดประเภททางการเงินตามลำดับความสำคัญ

Staff turnover:

At SDS, the staff turnover is less than 5%. The guards have many benefits and strong support that make SDS reliable and the guard confident.



0105554066126

บริษัทรักษาความปลอดภัยไดมอนด์เสิร์วสิสเซ็สเซ็สเซ็
SECURITY DIAMOND SERVICES Co. Ltd.

85 ถนนศรีเวียง แขวงสีลม เขตบางรัก กรุงเทพฯ 10500
85 Sri Wiang Road, Khwaeng Silom, Khet Bangrak, Bangkok 10500

GET IN TOUCH WITH US



+662-630-2536



sds-th.com



+669-9226-8614



ceo-sds