

# Savoir recevoir des visiteurs

tout en protégeant son patrimoine



## LE PARCOURS DE NOTORIÉTÉ

Si l'accueil de visiteurs est un outil de rayonnement, il peut toutefois constituer un formidable vecteur de captation d'informations stratégiques, notamment pour les **concurrents** et les **délégations étrangères**.

## SOMMAIRE

AVERTISSEMENT .....	2
INTRODUCTION.....	2
DÉFINITION.....	3
DÈS À PRÉSENT ET QUELLE QUE SOIT LA VISITE – SE PRÉPARER.....	4
AVANT LA VISITE - COMMUNIQUER .....	9
LA VEILLE DE LA VISITE – VÉRIFIER .....	12
LE JOUR DE LA VISITE – OBSERVER .....	16
APRÈS LA VISITE – CONTRÔLER.....	18

# AVERTISSEMENT

Le présent document n'a pas vocation à traiter de la tenue d'une réunion de travail, d'une conférence, d'un exercice ou de la présentation de matériels **impliquant l'accès de ses participants à des informations et supports classifiés (ISC)**. Celle-ci relève des dispositions prévues par l'IGI 1300\*, partie 5.4 et son annexe 35, auxquelles il convient de se reporter.

Ce document comprend deux grandes parties :

- Se préparer d'une manière générale, quelle que soit la visite ;
- Se préparer pour une visite spécifique (en amont, la veille, pendant et après la visite).

## INTRODUCTION

Le secteur industriel français de pointe est confronté à un risque de prédation des savoirs et savoir-faire stratégiques dans un contexte hyperconcurrentiel qui, au-delà du risque pour l'entreprise, peut également menacer les intérêts souverains de la nation. Dans ce cadre, la prise en compte du risque de captation d'informations sensibles lors de visites apparaît indispensable, tout particulièrement lors de la visite de délégations étrangères.

*\*Instruction Générale Interministérielle n° 1300/SGDSN/PSE/PSD du 09 août 2021 sur la protection du secret de la défense nationale.*

# DÉFINITION

Le **PARCOURS DE NOTORIÉTÉ**, également appelé « parcours de visite », est un circuit préétabli avec votre chargé de sûreté afin d'informer en amont les collaborateurs internes, d'assurer la sécurité de la visite de personnes étrangères à l'entité ainsi que de préparer le programme de cette visite. Ce parcours permet de transmettre une image professionnelle et maîtrisée de votre organisme tout en évitant l'accès à des informations sensibles et des locaux confidentiels ou sensibles.

Ce parcours de notoriété est, par ailleurs, obligatoire dans le cadre de la mise en œuvre de la protection du potentiel scientifique et technique de la nation (PSTN) dans une entreprise.

Il doit nécessairement comporter :

- **des mesures organisationnelles** visant à gérer les visiteurs au sein de l'établissement, de la préparation de leur venue jusqu'à leur départ, tout en assurant leur sécurité ainsi que celle du personnel du site ;
- **des mesures humaines** visant à impliquer et sensibiliser les employés sur les bonnes pratiques en matière d'accueil des visiteurs mais également sur les risques de fuites d'informations sensibles et le signalement de comportements inhabituels ;
- **des mesures techniques** visant à limiter la captation d'informations, de savoirs et de savoir-faire stratégiques et plus simplement le vol de matériels ou de documents.



# DÈS À PRÉSENT ET QUELLE QUE SOIT LA VISITE – SE PREPARER

## Mesures organisationnelles

- **identifier la sensibilité des locaux, des zones et des systèmes mis en œuvre** en fonction du préjudice qu'engendrerait la divulgation de savoir-faire ou de certaines informations, la perte ou la destruction des valeurs matérielles et immatérielles de l'établissement ;
- **réaliser une analyse de risques sûreté et appliquer des mesures de protection adaptées** à chacune des valeurs identifiées ;

Pour l'analyse de risques, s'appuyer sur le **Guide Pratique Analyse de Risques** de la direction du renseignement et de la sécurité de la défense (DRSD), librement téléchargeable sur le site internet de la DRSD.

Pour la protection des valeurs numériques, s'appuyer sur le guide d'hygiène informatique de l'ANSSI.

- **définir un ou plusieurs circuits de visite, dit « de notoriété », excluant les zones ou les locaux hébergeant les activités et systèmes les plus confidentiels ou sensibles**, en fonction du besoin d'en connaître des visiteurs. Prendre en compte les retours d'expérience des précédentes visites pour optimiser les différents circuits ;

Un client ne devrait pas forcément passer devant une pièce fabriquée pour un de ses concurrents.

- **intégrer ou compléter la procédure d'accueil des visiteurs dans le règlement intérieur en vous aidant de la présente fiche** ;
- **tracer le cheminement des circuits de visite sur un ou plusieurs documents comportant des plans schématiques des locaux**. Sécuriser ces documents et définir les acteurs y ayant accès. En faire mention dans le règlement intérieur sans les annexer à ce dernier ;
- **prendre en compte la présence des visiteurs dans le cadre de la prévention des risques professionnels**, notamment dans le document unique d'évaluation des risques professionnels (DUERP) ;
- s'il n'en existe pas, **mettre en place un registre « VISITEURS »** au format papier ou numérique. La mise en œuvre de ce registre nominatif sera en conformité avec la législation en vigueur sur la protection des données à caractère personnel, notamment s'agissant des obligations d'information, de droit d'accès et de sécurisation de ces données nominatives ;

- sensibiliser régulièrement les salariés au traitement d'un visiteur égaré et les différents acteurs concernés par ces visites (directions commerciales, communication, pôle visite, agents d'accueil, agent privé de sécurité, etc.).

## Mesures techniques

---

- identifier des lieux dédiés et adaptés à l'accueil des délégations, en fonction de leur nombre, de leur sensibilité et du besoin d'en connaître ;
- si possible, mettre en place un dispositif numérique (moyen de projection, PC, etc.) dédié aux visites sans interconnexion avec les systèmes d'information (SI) de l'entité.

### STATIONNEMENT

- idéalement, les places de stationnement des visiteurs à l'intérieur du site seront sous la surveillance directe du chargé d'accueil ou du poste de sécurité, sinon sous surveillance indirecte via des caméras de vidéosurveillance. Le stationnement sera clairement signalisé et fléché dès l'entrée du site pour éviter toute excuse pour des visiteurs un peu trop curieux.

### SALLE DE RÉUNION

- si possible, elle sera **dépourvue de vitres intérieures donnant sur des bureaux sensibles** (R&D par exemple). Des toilettes seront à proximité immédiate ;
- le cas échéant, installer (si possible) **des rideaux ou des stores aux vitres intérieures** ;
- **vérifier l'insonorisation de la salle, de sorte qu'il ne soit pas possible** de surprendre une conversation provenant du couloir, d'un bureau voisin ou d'une salle de repos ;
- **ne laisser aucune prise d'accès physique au réseau informatique interne accessible à tous**, l'idéal étant que les accès soient bloqués ;
- **ne pas afficher les codes de connexion au WIFI de l'entreprise** ;
- dans l'idéal, **prévoir un point d'accès WIFI destiné aux visiteurs et indépendant** du reste du réseau d'entreprise ;
- si nécessaire et si possible, **identifier plusieurs salles de réunion au sein des locaux ou bâtiments** ;
- **apposer un affichage rappelant l'interdiction de prises de vues photographiques et de captations sonores et vidéo** ;
- si possible, **mettre en place des casiers à l'extérieur de la salle de réunion, permettant aux visiteurs de déposer les téléphones et objets connectés.**

## SUPPORTS NUMÉRIQUES

- **si possible, prévoir un ordinateur dédié aux visites, non connecté au réseau et sans aucune donnée sensible autre que les documents devant être présentés**, permettant, le cas échéant, de recevoir les supports amovibles des visiteurs ;

Exemple : des visiteurs prétextent la panne de leur ordinateur portable pour solliciter la mise à disposition d'un ordinateur pour y connecter leur clé USB... celle-ci pouvant parfois contenir un logiciel particulièrement intrusif.

- **prévoir systématiquement une clé USB dédiée aux visites, par exemple pour échanger des documents commerciaux volumineux**. Elle ne comportera aucun autre fichier que ceux devant être échangés. Elle ne restera jamais sans surveillance. Avant toute connexion sur le SI d'entreprise, vérifier l'innocuité de cette clé sur une station blanche à jour ;
- tout support externe à l'entité devra passer par une station blanche. Les ordinateurs et clés utilisés devront être contrôlés a posteriori par le service informatique.

### ÉGALEMENT...

- **étudier la possibilité de placer sous vidéosurveillance le ou les circuits de visite** dans le respect de la réglementation en vigueur ;

S'aider pour cela des fiches d'information sur la vidéosurveillance de la CNIL : [www.cnil.fr](http://www.cnil.fr)

- **le cas échéant, prévoir des rideaux ou des stores pour tous les bureaux, locaux ou zones vitrées sensibles donnant sur les cheminements intérieurs du ou des circuits de visite**. Ils seront utilisés en fonction de la délégation ;

Il est, en effet, parfois impossible d'identifier plusieurs circuits lorsqu'il n'existe qu'un seul couloir dans l'établissement.

- **vérifier que le matériel informatique ou tout support sensible** (ex. plan des laboratoires ou rétroplanning d'un projet) **est disposé de façon à éviter toute captation à la simple vue des mots de passe et informations sensibles lors de la visite**. Tourner par exemple les ordinateurs de manière à empêcher la visibilité de l'écran et du clavier ;
- **si ceux-ci n'existent pas encore, prévoir des badges « VISITEUR »**. N'inscrire aucune autre mention que « VISITEUR » sur le badge, qui peut être un simple papier inséré dans un porte-badge en plastique. Ces badges seront récupérés à l'issue de la visite ;
- **s'il s'agit d'un badge d'accès électronique sans contact, ne donner aucun droit ou seulement des droits d'accès très restreints aux locaux**, par exemple uniquement un droit pour un passage non gardé (PNG) intérieur installé au niveau de l'accueil. Ne

jamais oublier qu'un simple smartphone peut permettre de recopier très facilement des badges utilisant certaines technologies obsolètes ;

Fournir un tour de cou d'une couleur différente de celui des employés. Préférer toujours un tour de cou à une épingle ou un dispositif rétractable pour le port du badge. À noter que le tour de cou peut être utilement remplacé par un casque ou une chasuble marquée « VISITEUR » d'une couleur différente de celle des employés.

- **apposer tout au long du ou des circuits de visite un affichage rappelant l'interdiction de prises de vues photographiques** et de captations sonores et vidéo, tout particulièrement au niveaux des accès et surtout du ou des showrooms ;
- si possible, **déplacer les imprimantes non sécurisées** (n'utilisant pas un code d'accès ou une authentification par badge par exemple) implantées sur l'ensemble du ou des circuits de visite ;
- envisager la possibilité de **matérialiser le cheminement du parcours de notoriété** (fléchage, ligne de vie, limites séparant d'une machine-outil et de sa zone de travail, etc.) ;
- dans tous les cas, ne jamais laisser un visiteur seul dans les locaux.

## Mesures humaines

---

**Dans le cadre de la gestion des visites, identifier les personnes suivantes :**

- **un responsable de visite** gérant la délégation (prise en charge des visiteurs, de leur arrivée à leur départ). Ce responsable peut s'appuyer sur le chargé de communication si ce dernier existe au sein de l'établissement ;
- **si possible, deux personnes d'encadrement** accompagnant les visiteurs lors des déplacements, dont une dans l'idéal étant « serre-file ». Ce nombre pourra être plus important en fonction de la taille de la délégation.

Lors des déplacements dans les locaux, il est important de toujours disposer d'un personnel d'encadrement dédié à l'accompagnement des visiteurs voulant se rendre aux toilettes ou à leurs véhicules. L'expérience montre que les toilettes ne sont pas toujours à proximité, le véhicule non plus.

**En fonction de la délégation, ces personnes seront, le cas échéant, assistées par :**

- **le responsable sûreté chargé de l'accueil de la délégation** dès l'arrivée de celle-ci sur le parking du site ou au poste de filtrage à l'entrée du site ;
- **l'agent d'accueil en charge de la vérification de l'identité des visiteurs** et de la gestion des badges « VISITEUR », voire, le cas échéant, des équipements de protection ;
- **l'agent de sécurité en charge du suivi en temps réel du déplacement de la délégation** dans les locaux de l'entreprise, via les images de vidéosurveillance.

# AVANT LA VISITE - COMMUNIQUER

## Mesures organisationnelles

---

### CONCERNANT LES VISITEURS

- **se renseigner sur l'objectif précis de la visite, à plus forte raison s'il s'agit d'une délégation étrangère :**
  - quel est l'objectif de la visite ?
  - la visite consiste-t-elle à dérouler un questionnaire selon un référentiel précis ? Si oui, lequel ?
  - quelles sont les thématiques ou les technologies qui intéressent la délégation ?
  - qui sont les interlocuteurs (nom, fonction, nationalité, etc.) ?

Ces informations permettent de restreindre l'accès physique aux seuls locaux et bureaux nécessaires mais également de se renseigner sur l'entreprise.

- **se faire transmettre plusieurs jours avant la visite, les biodatas de toutes les personnes présentes lors de la visite, y compris, le cas échéant, du traducteur** (photo d'identité, nom, prénoms, date et lieu de naissance, nationalité, fonction précise au sein de l'entreprise) ;

Toujours adapter le nombre de visiteurs à la configuration des locaux et à l'effectif disponible le jour de la visite. Moins ils seront nombreux, plus il sera facile de les encadrer.

- **informer le référent local de la DRSD de la visite de cette délégation, en particulier pour une délégation étrangère ;**
- **le cas échéant, se faire transmettre la pointure des visiteurs en cas de port obligatoire de chaussures ou de coques de sécurité** lors de la visite ;

Toujours privilégier le prêt des chaussures ou des coques de sécurité. En fonction de l'activité de l'entreprise, il peut être très instructif pour certains visiteurs de réaliser des prélèvements par contact sur des résidus présents au sol. **L'expérience montre également que certains visiteurs n'hésitent pas à tremper leur cravate dans des solutions liquides trop facilement accessibles pour en prélever des échantillons...**

- **informer le représentant de la délégation, dès les premiers échanges, sur les conditions d'accueil et l'obligation de confidentialité des membres de la délégation**, en précisant par exemple les éléments suivants :
  - les personnes non déclarées préalablement ou qui ne pourront présenter une pièce d'identité officielle le jour même ne pourront pas être accueillies dans les locaux de l'entreprise. Aucune exception ne sera possible ;

Exemple : certaines délégations étrangères comprennent, à la demande du pays concerné, des membres de ses services de renseignement rajoutés au dernier moment.

- en échange d'une pièce d'identité officielle, un badge « VISITEUR » sera remis. Ce dernier devra être porté de manière apparente tout au long de la visite. La pièce d'identité sera restituée après récupération du badge ;
- il pourra éventuellement être demandé à ce qu'un engagement de confidentialité soit signé par les visiteurs ;
- les membres de la délégation seront systématiquement accompagnés lors de la visite pour des raisons de sécurité ;
- les prises de vues photographiques, les captations vidéo et audio mais également les manipulations de matériels sensibles exposés seront strictement interdites lors de la visite. Des exceptions seront toutefois possibles après autorisation de la direction ;
- le cas échéant, smartphones, appareils photo, lunettes et appareils connectés seront sécurisés dans des casiers ou dans des sacs opacifiants mis à la disposition des visiteurs dès leur arrivée sur le site.

Se rappeler qu'il existe des lunettes de soleil ou de vue de plus en plus performantes permettant de capter des images et du son. Ces lunettes disposent d'une commande vocale pour certaines. Il sera donc nécessaire de s'interroger en présence d'un porteur de lunettes marmonnant seul, touchant régulièrement les branches de celles-ci, voire les retirant ou les enlevant tout au long de la visite. Pour certaines, la présence de minicapteurs vidéo parfaitement visibles aux extrémités des branches de la lunette devrait systématiquement obliger son porteur à les retirer.

## EN INTERNE

- **informer la chaîne de sécurité/sûreté de la visite de toute délégation ;**
- **s'assurer que la visite d'une autre délégation ce jour-là ne prête pas à conséquence dans l'organisation et qu'elles ne sont pas concurrentes au plan commercial.** De manière générale, éviter d'accueillir plusieurs délégations le même jour ;
- **le cas échéant, identifier le circuit de visite le plus approprié ;**
- **s'assurer du bon fonctionnement de l'ensemble des dispositifs de sûreté et de sécurité** indispensables au bon déroulement de la visite, tout particulièrement les contrôles d'accès et la vidéosurveillance ;
- **identifier et vérifier les disponibilités des intervenants**, répartir les rôles ;
- **définir des éléments clairs de langage**, notamment sur des sujets que la direction ne souhaite pas voir être abordés. Il est tout à fait possible de prévoir de mettre fin à un échange sur directives de la direction pour des raisons de confidentialité. Enfin, si une telle situation devait se présenter, **informer**, si possible immédiatement, **le responsable de la visite ;**

- **rappeler le besoin d'être vigilant aux questions posées et aux échanges libres ;**
- **rappeler les consignes à suivre pour guider un visiteur « égaré ».**

# LA VEILLE DE LA VISITE – VÉRIFIER

## Mesures organisationnelles

---

Contrôler physiquement le circuit de visite en prenant en compte les points suivants :

- ❑ **s'assurer de l'absence d'objets ou de documents sensibles librement accessibles ou trop visibles** : process industriel sensible, plans de fabrication, documents restés sur les imprimantes, poubelles non vidées, etc. ;
- ❑ **s'assurer que le matériel informatique et les supports sensibles sont disposés de façon à éviter toute vue ou prise de vue** ;
- ❑ si possible, **matérialiser le cheminement du parcours de notoriété** (fléchage, ligne de vie, limites séparant d'une machine-outil et de sa zone de travail, etc.) ;
- ❑ le cas échéant, **s'assurer du verrouillage des vitrines présentant des prototypes ou des produits sensibles**. Au besoin, retirer ou dissimuler certains objets ou panonceaux trop explicites (par exemple « *Pièce XX du moteur de telle SOCIÉTÉ* »).

Prendre en compte les éléments suivants dans la salle de réunion :

- ❑ **contrôler l'absence d'objets ou d'informations sensibles** (ex. plan) ;
- ❑ le cas échéant, **s'assurer que le tableau blanc est soigneusement effacé**, que le **paperboard ne contient aucune page annotée sensible** et que les post-it sont retirés ;

Exemple : il suffit de tourner quelques pages du paperboard présent dans la salle pour retrouver les traces des dernières réunions. Idéalement, ne pas utiliser ce type de support en temps normal, uniquement en cas d'urgence (coupure d'alimentation électrique par exemple).

- ❑ **s'assurer que les poubelles sont vidées** ;
- ❑ **s'assurer du bon fonctionnement de l'ordinateur dédié** et du matériel de projection ;
- ❑ **s'assurer que la session de l'ordinateur s'ouvre avec un mot de passe et que celui-ci n'est pas inscrit sur un post-it** ;
- ❑ **s'assurer de l'absence de fichiers sensibles ou de fichiers en lien avec une précédente délégation sur l'ordinateur**. Le cas échéant, se rapprocher du service informatique pour une suppression sécurisée des fichiers ;
- ❑ **fermer les dossiers et messageries** ;

- ❑ **installer le diaporama de présentation sur l'ordinateur** et vérifier son bon fonctionnement. Configurer l'ordinateur de manière à étendre les écrans et utiliser le mode présentateur pour éviter d'afficher tous les fichiers ouverts ou ceux présents sur le bureau ;
- ❑ **éteindre autant que possible les systèmes d'information sans rapport avec la visite.** Pour ceux devant rester en fonctionnement, s'assurer qu'ils ne sont pas facilement accessibles aux visiteurs.

**Ne jamais négliger ces dernières mesures.** Trop souvent le responsable **se connecte au réseau sur son compte, avec son propre ordinateur**, sous les yeux de l'auditoire pour diffuser la présentation. Il devient alors très facile de **capter des informations** sur l'écran de projection (login de connexion, nom de fichier explicite, fond d'écran parfois très personnel, pop-up d'un nouvel e-mail, etc.).  
Pouvant apparaître anodines prises isolément, ces informations peuvent toutefois être sensibles mises bout à bout.

#### Effectuer les vérifications suivantes :

- ❑ **s'assurer que le chargé d'accueil dispose des biodatas des membres de la délégation ;**
- ❑ **s'assurer que le registre « VISITEURS » au format papier n'est pas resté à l'accueil** en libre accès (risque de captation d'informations sur les clients) ;
- ❑ **s'assurer que les badges « VISITEUR » sont prêts** et, le cas échéant, correctement configurés ;
- ❑ **le cas échéant, s'assurer du nombre suffisant de chaussures ou de coques de sécurité**, voire de bouchons d'oreilles, de casques et de lunettes de protection ;
- ❑ **rappeler le rôle de chacun des acteurs de la visite**, du responsable de visite aux encadrants et agents privés de sécurité le cas échéant, les consignes à respecter ainsi que le déroulé de la visite. Ceci inclut les modalités relatives aux pauses déjeuner, le cas échéant ;
- ❑ **sensibiliser et responsabiliser les acteurs de la visite en amont sur les risques existants.** Rappeler l'importance de l'application des consignes et s'assurer qu'elles sont parfaitement comprises ;
- ❑ **rappeler les consignes concernant les questions intrusives**, notamment stopper immédiatement l'échange pour des raisons de confidentialité et en informer le responsable de la visite ;
- ❑ **mettre à disposition un point de contact et une procédure pour remonter tout incident, y compris en cas de simple doute.**

### Quelques exemples de consignes :

- ❑ **rester en permanence vigilant**, particulièrement lors des déplacements propices à la captation d'informations ;
- ❑ **rester méfiant lors de la remise de cadeaux**. Il existe un risque de corruption ou de piégeage via les objets promotionnels ;
- ❑ **rendre compte sans délai au responsable de la visite**, de la sécurité ou de la direction de tout problème ou événement inattendu survenant lors de la visite.

### Rappeler aux acteurs de la visite les quelques situations inhabituelles, anormales ou suspectes suivantes :

- ❑ visiteur posant des questions très intrusives sur l'activité de l'entreprise ;
- ❑ visiteur prétextant la panne de son ordinateur portable pour solliciter la mise à disposition d'un ordinateur de l'entreprise ;
- ❑ visiteur insérant une clé USB sur un ordinateur/machine de l'établissement sans autorisation ;
- ❑ visiteur sollicitant la possibilité de recharger son smartphone sur un ordinateur connecté au réseau ;
- ❑ visiteur prenant des photographies sans autorisation ;
- ❑ visiteur manipulant des produits sensibles ou des machines sans autorisation ;
- ❑ visiteur trempant volontairement un vêtement dans une solution liquide ;
- ❑ visiteur ne portant visiblement pas le badge « VISITEUR » autour du cou ;
- ❑ visiteur s'absentant de la salle de réunion de longues minutes pour téléphoner ;
- ❑ visiteur s'écartant discrètement du groupe lors de la visite des locaux ;
- ❑ visiteur dont l'orthographe du nom n'est pas exactement la même que celle du visiteur annoncé et prétextant une erreur dans la transmission des informations ;
- ❑ de manière générale, tout visiteur ne respectant pas les consignes et adoptant un comportement étrange ou suspect ;
- ❑ disparition de documents ou de matériels après la visite ;
- ❑ absence de restitution des chaussures ou coques de sécurité.

### Enfin, rappeler à l'ensemble du personnel susceptible de croiser la délégation les consignes suivantes :

- ❑ **observer une vigilance particulière à ce moment précis** ;
- ❑ **raccompagner systématiquement un visiteur seul** semblant chercher son chemin vers le groupe et rendre compte immédiatement. Rappeler au besoin les coordonnées du responsable à prévenir ;
- ❑ **rester discret dans les espaces communs en présence des visiteurs**. Ne pas s'engager dans des conversations sensibles ou confidentielles ;

- **garder à l'esprit qu'une délégation étrangère peut comprendre une conversation ;**
- **toujours verrouiller une session informatique avant de quitter le poste et fermer la porte en sortant d'un bureau.**

# LE JOUR DE LA VISITE – OBSERVER

## Mesures organisationnelles

- ❑ **s'assurer que les biodatas de tous les membres de la délégation correspondent à celles transmises. Respecter strictement les règles de refus d'accès au site en cas de situation non conforme ;**
- ❑ **s'assurer que le porteur de la pièce d'identité soit le bon détenteur ;**
- ❑ **renseigner le registre « VISITEURS » en inscrivant : nom, prénom, société, fonction et horaires d'entrée et de sortie de ces derniers. Garder ces informations un délai minimum (un mois par exemple) sans pour autant les conserver trop longtemps ;**

Ne jamais laisser les visiteurs renseigner eux-mêmes le registre.

Outre le respect de la réglementation RGPD, il existe un risque d'y mentionner de fausses identités ou de capter des informations sur les clients du site visité. C'est d'autant plus vrai s'il est possible de remonter plusieurs années en arrière sur ce registre.

- ❑ **en échange d'une pièce d'identité officielle, remettre un badge « VISITEUR ». Rappeler l'obligation de son port apparent ;**
- ❑ **idéalement, prendre en charge les membres de la délégation dès l'arrivée sur le parking ou depuis le poste de filtrage afin d'éviter toute déambulation sur les espaces extérieurs. Les accompagner en permanence, de leur arrivée au départ du site.** Eviter de scinder la délégation tout au long de la visite. Ne jamais laisser un visiteur sans surveillance ;
- ❑ **notifier en anglais, ou dans la langue des visiteurs si cela est possible, l'importance du respect des consignes, de l'interdiction des prises de vues photographiques au suivi scrupuleux du circuit de visite préétabli. Rappeler également les engagements de confidentialité propres à la visite. Il est également possible d'annoncer l'exclusion immédiate de tout contrevenant à ces consignes ;**
- ❑ **interdire la connexion d'équipements et de supports amovibles détenus par les visiteurs à des postes reliés au système d'information de l'entreprise (clés USB, disques durs externes, smartpone, etc.) ;**
- ❑ **en cas d'utilisation d'un ordinateur dans la salle de réunion, s'assurer qu'il est orienté de manière à empêcher la visibilité du clavier par les visiteurs. Projeter l'image uniquement après avoir ouvert la présentation sur cet ordinateur, jamais avant ;**
- ❑ **interdire l'usage d'objets connectés dans les lieux sensibles ;**

- **interdire la prise de photos et vidéos par les visiteurs.** Pour les visites de journalistes, les angles de prises de vues doivent être définis à l'avance et vérifiés lors de la réalisation. Toutes les productions doivent faire l'objet d'une vérification in situ en fin de reportage ;
- **idéalement prendre le café d'accueil dans la salle de réunion** et non dans l'espace de convivialité du site ;
- **rester vigilant aux questions posées et aux échanges libres ;**
- **ne jamais laisser les outils de travail des intervenants sans surveillance dans la salle de réunion** (mallette, ordinateurs portables, téléphones, etc.) ;
- **ne jamais laisser un membre de la délégation seul dans la salle de réunion**, même quelques minutes, qui plus est si, exceptionnellement, un ordinateur connecté au réseau de l'entreprise est présent ;
- **fermer systématiquement la porte de la salle de réunion** en présence de la délégation ;
- **ne jamais prêter ses supports amovibles à un visiteur**, autre que la clé USB dédiée à cela ;
- **ne jamais flasher un « QR code » proposé par un visiteur.** Ce dernier peut renvoyer vers une application ou un site malveillant ;
- si possible, assurer **en temps réel le suivi de la délégation lors de ses déplacements dans les locaux** via les images des caméras de vidéosurveillance renvoyées au poste de sécurité.

## **EN CAS DE QUESTIONS TROP INTRUSIVES OU D'INCIDENTS LORS DE LA VISITE**

- **se référer aux consignes définies à l'avance en cas de questions récurrentes et intrusives ;**
- en fonction de la situation, **mettre fin à l'échange en évoquant une consigne de confidentialité définie par la direction ;**
- **informer le responsable de la visite. Au besoin, mettre fin à la visite ;**
- **en fonction, déposer plainte auprès de l'unité des forces de sécurité intérieure territorialement compétente** (commissariat de la police nationale ou brigade de la gendarmerie nationale) ;
- **informer le référent de la DRSD.**

# APRÈS LA VISITE – CONTRÔLER

## Mesures organisationnelles

---

- **si possible et en fonction du type de visite, refaire le circuit de visite pour s'assurer de l'absence d'éléments inhabituels** (disparition d'objets ou de documents, comportement suspect, etc.) ;
- **demander au personnel de rendre compte de tout fait qui aurait suscité l'étonnement lors de la visite de la délégation.**

### Le cas échéant :

- **contrôler les ordinateurs/supports numériques auxquels les membres de la délégation auraient eu accès ;**
- **faire vérifier par le responsable sécurité des SI tous les supports numériques, telles que les clés USB, qui ont été utilisés ou offerts en cadeau.**



**PRÉPARATION**  
**COMMUNICATION**  
**OBSERVATION**  
**VÉRIFICATION**  
riment toujours avec  
**DÉLÉGATION**