Annexe technique d'intervention

Dans le cadre de ses interventions, l'administrateur des systèmes d'information peut être amené à se substituer à un utilisateur ou à manipuler des informations sensibles ou des matériels propres à celui-ci. Le présent document complète la charte des administrateurs en précisant les procédures à respecter lorsque l'administrateur est confronté aux situations décrites.

Si l'administrateur fait face à une situation non décrite dans ce document et qu'il estime insuffisamment encadrée par les articles de la charte, il doit la porter à la connaissance du responsable de la sécurité des systèmes d'information pour qu'elle soit ajoutée après validation.

De l'utilisation des profils et des comptes

Substitution à un utilisateur

Contexte

Suite à un problème lié à une application, la demande nécessite d'utiliser un compte de substitution car il n'y a pas d'autre méthode ou télémaintenance possible, pour visualisation uniquement.
Si la demande est formulée par téléphone, l'administrateur doit inviter le demandeur à utiliser le formulaire du P@C ou à envoyer un courriel pour que celle-ci soit instruite.

Recevabilité

La demande doit être formulée par l'interface web du point d'accueil centralisé ou par courriel.

Modalités d'intervention autorisées

- Utilisation d'un compte générique de substitution ayant à minima les droits de l'utilisateur.
- Utilisation d'une authentification forte par OTP lié au compte de l'utilisateur.
- Utilisation du couple identifiant/mot de passe de l'utilisateur. Une fois l'intervention terminée, l'utilisateur doit être informé de l'obligation qui lui incombe de modifier son mot de passe.

L'utilisateur doit être informé qu'aucune modification ne pourra être apportée sur l'application.

Preuve

- Si la demande est déposée par le formulaire web du point d'accueil centralisé, le ticket vaut preuve.
- Si la demande est formulée par courrier électronique, l'identité du demandeur doit être vérifiée et une réponse explicite de prise en charge doit lui être adressée. La copie de cet échange doit être conservée.

La preuve de la demande doit être complétée par la description chronologique de l'intervention. Doivent au moins y figurer l'identité du demandeur et l'objet de sa demande, la date et l'heure de début et de fin de l'intervention, la mention de l'information portée à la connaissance de l'utilisateur et tout élément constaté qui apparait pertinent à l'administrateur.

Création et réinitialisation d'un couple identifiant/mot de passe

Contexte

L'administrateur répond à une demande de création d'un compte ou de réinitialisation d'un mot de passe. Il a alors connaissance du mot de passe de l'utilisateur.

Recevabilité

- La demande de création ou de réinitialisation peut être formulée par l'interface web du point d'accueil centralisé ou par courriel.
- La nécessité de réinitialisation d'un mot de passe peut résulter du processus de traitement des comptes compromis ou incidents SSI.
- La demande de création d'un nouveau compte utilisateur doit être approuvée par le responsable hiérarchique du nouvel agent ou le responsable du traitement auquel le compte ouvre un accès.
- Lorsque la demande est transmise par courriel, l'identité de la personne et la validité de la demande doivent être vérifiées.

Modalités d'intervention autorisées

Lors d'une création, l'administrateur génère un couple identifiant/mot de passe qu'il communique à l'utilisateur. Sauf en cas de contact direct avec l'utilisateur, les deux éléments ne doivent pas lui être communiqués par le même canal.

Lors d'une réinitialisation par l'administrateur, celui-ci génère un nouveau mot de passe qu'il communique à l'utilisateur.

Dans les deux cas l'administrateur informe l'utilisateur qu'il doit modifier son mot de passe. Si ce dernier de connait pas le mode opératoire pour modifier son mot de passe, l'administrateur le lui communique ou lui indique où trouver l'information.

Preuve

- Si la demande est déposée par le formulaire web du point d'accueil centralisé, le ticket vaut preuve.
- Si la demande est formulée par courrier électronique, l'identité du demandeur doit être vérifiée et une réponse explicite de prise en charge doit lui être adressée. La copie de cet échange doit être conservée.

La preuve de la demande doit être complétée par la description chronologique de l'intervention. Doivent au moins y figurer l'identité du demandeur et l'objet de sa demande, la date et l'heure de début et de fin de l'intervention, la mention de l'information portée à la connaissance de l'utilisateur et tout élément constaté qui apparait pertinent à l'administrateur.

Demande d'accès à un environnement ou un compte utilisateur

Contexte

L'administrateur reçoit d'un tiers une demande d'accès à l'environnement d'un utilisateur ou de communication du couple identifiant / mot de passe d'un utilisateur.

Recevabilité

- La demande doit être formulée par l'interface web du point d'accueil centralisé. Toute autre forme n'est pas recevable, le demandeur doit alors être aiguillé vers le dépôt web.
- La demande doit émaner du responsable hiérarchique de la personne, ou être validée par lui.
- La demande doit être motivée par un impératif de service (absence de longue durée, mutation d'un agent, etc.). L'administrateur s'assurera du caractère raisonnable et des circonstances de la demande.
- Sauf cas de force majeure, l'utilisateur doit avoir été informé au préalable de cette demande le concernant, la copie de cet échange doit être jointe aux éléments de preuve.
- Le RSSI doit être informé de cette demande.

Modalités d'intervention autorisées

L'administrateur fournit un accès ou le couple identifiant/mot de passe sous couvert d'une personne responsable :

- Chef de pôle / chef de service.
- Responsable / directeur.
- Chef d'établissement / gestionnaire / agent comptable.

L'administrateur rappelle les règles au destinataire de l'accès :

- Respect de la vie privée : les documents et messages explicitement privés ne doivent pas être ouverts ni copiés ou transférés.
- Les informations personnelles involontairement consultées lors des opérations permises doivent rester strictement confidentielles.

L'administrateur informe l'agent dont l'accès a été divulgué de la nécessité de modifier son mot de passe dès son retour. Il s'assure que celui-ci y a bien procédé.

Preuve

- Le ticket de demande déposé par le formulaire web du point d'accueil centralisé doit être complété par la copie de l'information de l'utilisateur dont l'accès est divulgué.
- La preuve de la demande doit être complétée par la description chronologique de l'intervention, notamment la mention des informations portées à la connaissance de tous les utilisateurs concernés ainsi que tout élément constaté qui apparait pertinent à l'administrateur.

Des interventions sur les matériels

Intervention sur un matériel privé

Contexte

L'administrateur intervient sur un équipement personnel privé.

Recevabilité

- La demande doit être formulée par l'interface web du point d'accueil centralisé. Toute autre forme n'est pas recevable, le demandeur doit alors être aiguillé vers le dépôt web.
- L'intervention peut être rendue nécessaire en cas de migration, transfert, mise à jour suite à une intervention antérieure justifiée.
- L'intervention sur matériel privé doit être approuvée par le supérieur hiérarchique de l'administrateur.
- L'autorisation expresse du propriétaire du matériel doit être recueillie au préalable, selon le modèle ci-dessous.
- Le propriétaire fixe librement la durée de l'autorisation, toutefois celle-ci est révoquée dès lors que la personne quitte le périmètre de responsabilité de l'administrateur (changement de fonction, mutation, départ).

Autorisation d'intervention sur matériel personnel

M/Mme nom : Prénom : autorise

M/Mme nom : Prénom : dans le cadre de ses fonctions d'administrateur

à intervenir sur le matériel personnel décrit ci-après :

Décrire l'intervention prévue :

Exposer les raisons nécessitant cette intervention :

Durée de validité de ce document :

M/Mme : Signature : Date :

Modalités d'intervention autorisées

L'administrateur procède strictement à l'intervention prévue par l'autorisation.

Preuve

- Le ticket de demande déposé par le formulaire web du point d'accueil centralisé doit être complété par la copie de l'autorisation.
- La preuve doit être complétée par la description chronologique de l'intervention, notamment la mention des informations portées à la connaissance du propriétaire de l'équipement ainsi que tout élément constaté qui apparait pertinent à l'administrateur.