Directive concernant l'utilisation des ressources informatiques à la Haute école spécialisée bernoise

Le recteur de la Haute école spécialisée bernoise (BFH),

vu l'art. 35, al. 2, let. h de la loi du 19 juin 2003 sur la Haute école spécialisée bernoise (LHESB ; RSB 435.411),

arrête :

1 Dispositions générales

Art. 1 But et champ d'application

[1] Cette directive règle l'utilisation des ressources informatiques à la BFH par les personnes agréées.

[2] Elle s'applique à tous les utilisateurs et utilisatrices des ressources informatiques de la BFH.

Art. 2 Définitions

[1] *Les moyens informatiques* sont tous les appareils, équipements et programmes d'ordinateurs utilisés pour le traitement électronique d'informations, notamment :

- *a* les systèmes d'ordinateurs et smart devices ;
- *b* les appareils périphériques (imprimantes, disques externes, supports de stockage, etc.) ;
- *c* les réseaux (avec ou sans fil) ainsi que les appareils d'accès (routeurs, points d'accès WLAN, security devices, etc.) ;
- *d* les logiciels.

[2] Les informations sont des données factuelles et des données personnelles.

[3] Les données secondaires sont des informations sur l'utilisation de moyens informatiques.

[4] *Traiter* des données personnelles désigne le fait d'acquérir des informations, de les conserver, de les modifier, de les combiner, de les faire connaître ou de les détruire.

[5] *Faire connaître* désigne tout acte rendant accessibles des données personnelles, comme permettre une consultation, renseigner, transmettre ou publier.

[6] Les services informatiques sont les services régis par les IT-Services qui sont à disposition des utilisateurs et utilisatrices (p. ex. DNS, e-mail, annuaires), ainsi que les services et services informatiques régis par les départements qui sont assurés par des personnes œuvrant à la BFH ou pour le compte de la BFH.

[7] Les administrateurs et administratrices IT sont des personnes responsables du fonctionnement des services informatiques.

[8] Les ressources informatiques englobent les moyens informatiques, les informations et les services informatiques.

[9] *Les utilisateurs et utilisatrices* sont toutes les personnes se servant des ressources informatiques de la BFH, notamment :

- *a* les membres de la BFH, au sens de l'Ordonnance sur la Haute école spécialisée [1] ;
- *b* les personnels d'organisations externes qui, en tant que mandataires ou partenaires de la BFH, accomplissent des activités à la BFH ou pour la BFH (par ex. activités de recherche, de support, d'entretien ou de développement, etc.) ;
- *c* les membres d'autres établissements académiques avec lesquels existent des conventions ;
- *d* d'autres personnes prenant part à des évènements organisés par la BFH et utilisant les ressources informatiques de cette dernière pour une durée déterminée.

[1] RSB 436.811.

2 Utilisation de moyens informatiques à la BFH

Art. 3 Ressources informatiques

[1] Les ressources informatiques sont exclusivement utilisées pour les tâches confiées par la BFH.

[2] L'utilisation des ressources informatiques à titre privé, personnel et non commercial est autorisée tant qu'elle ne nuit pas à l'accomplissement des tâches liées au travail ou aux études, ni au fonctionnement du système informatique.

[3] L'utilisation de ressources informatiques pour l'accomplissement des tâches principales confiées par la BFH, en particulier l'enseignement et la recherche, prime toujours les autres utilisations.

[4] Les utilisations suivantes nécessitent une autorisation préalable du directeur ou de la directrice de département et du ou de la responsable des IT-Services :

a utilisation de ressources informatiques pour des activités privées à but lucratif (p.ex. SpinOff) ;

b utilisation de ressources informatiques nécessaires aux activités d'enseignement et de recherche, mais d'ordinaire interdites au sens de l'art. 7.

[5] L'utilisation des ressources informatiques par des unités organisationnelles n'appartenant pas à la BFH ainsi que l'utilisation selon l'al. 4, let. a sont règlementées dans des accords spécifiques.

[6] Lorsque des services informatiques ne sont pas régis par les IT-Services tout en étant réalisés au sein du réseau de la BFH ou pour la BFH, ils sont soumis aux mêmes exigences concernant la protection des données, les conditions d'utilisation et le stockage des données secondaires.

[7] Aucune modification des paramètres de sécurité et des logiciels ne peut être effectuée sur des appareils officiels, dotés d'un Clientsetup-BFH, qui sont fournis et entretenus par la BFH.

[8] Le vol d'appareils, de même que des observations quant à la sécurité des ressources informatiques doivent immédiatement être annoncés aux IT-Services et à la personne chargée de la sécurité.

[9] L'élimination d'informations enregistrées sur des supports de données est règlementée dans la « Directive BFH relative à l'élimination de supports de données et au traitement préalable des informations ».

Art. 4 Compte utilisateur

[1] L'accès aux ressources informatiques (sauf en cas de rares exceptions) n'est possible que par le biais du « compte utilisateur BFH » (identifiant et mot de passe).

[2] Le compte utilisateur est personnel et non transmissible.

[3] La personne inscrite comme titulaire de ce compte est tenue d'assurer la confidentialité de ses données et d'observer les mesures de précaution qui lui incombent.

[4] Si le ou la titulaire d'un compte utilisateur soupçonne que des personnes non autorisées y aient accès, il lui incombe d'en avertir immédiatement les IT-Services via le support IT.

Art. 4a Accès aux comptes utilisateurs

[1] L'accès direct au contenu du compte d'utilisateur, y compris à la boîte aux lettres électronique personnelle, par des personnes autres que la personne inscrite sur le compte n'est pas autorisé. Cette disposition ne s'applique pas aux interventions réalisées dans le champ de compétence des responsables de l'administration informatique, interventions au cours desquelles on veillera cependant tant que possible à ne pas divulguer les contenus.

[2] Les responsables hiérarchiques peuvent exiger que les employé-e-s rendent compte de leur correspondance électronique professionnelle et, en cas d'indices de manquements aux devoirs, prendre les mesures qui, en termes de droit du personnel, permettent de contrôler un compte d'utilisateur, tout en tenant compte des dispositions figurant à l'al. 6.

[3] En cas d'absence prolongée ou d'une durée imprévisible, les employé-e-s doivent configurer un message d'absence automatique. S'il fait défaut, le ou la responsable hiérarchique est en droit de le faire activer à leur place.

[4] Si l'on suppose que des données professionnelles nécessaires à l'exercice légal des fonctions se trouvent sur le compte utilisateur d'un ancien membre du personnel ou d'un membre du personnel

absent, il y a lieu de contacter cette personne et de lui demander, dans un délai imparti, de mettre les données à disposition sur le lieu de travail habituel de la BFH ou d'autoriser l'accès aux données du compte utilisateur.

[5] Si l'employé-e ou l'ancien-ne employé-e n'est pas joignable ou ne répond pas aux demandes au sens de l'al. 4, les données peuvent être consultées par le biais d'une mesure de substitution. Au moment où le délai pour satisfaire aux demandes est communiqué à la personne concernée, elle doit être informée de la mesure de substitution encourue en cas d'inaction de sa part. En cas de danger imminent ou s'il est évident que la personne concernée ne satisfera pas aux exigences en temps utile, une mesure de substitution peut s'appliquer sans octroi de délai.

[6] Tout accès aux données d'un compte utilisateur doit être proportionné et être effectué par le ou la responsable hiérarchique ou en sa présence. Les données privées et professionnelles doivent, dans la mesure du possible, être séparées afin que le contenu privé ne soit pas divulgué. Une fois l'accès effectué, la personne concernée doit être informée de l'heure, des démarches entreprises et des personnes qui étaient présentes.

Art. 5 Appareils informatiques privés ou auto-administrés

[1] Le recours à des appareils privés ou à des appareils auto-administrés par leurs utilisateurs ou utilisatrices est autorisé sous réserve de certaines restrictions.

[2] L'usage conforme de tels appareils est du ressort et de la responsabilité de leurs utilisateurs et utilisatrices.

[3] Les appareils privés ou auto-administrés ne peuvent être reliés au réseau (p. ex. BFH-LAN, BFH WLAN, VPN, etc.) que si les conditions suivantes sont remplies :

- *a* Tous les logiciels (système d'exploitation et applications) doivent être sécurisés par les dernières mises à jour disponibles.
- *b* Les logiciels utilisés sur l'appareil doivent être activement protégés par des mises à jour sécuritaires (pas de logiciel « End of Support / Life »).
- *c* Chaque logiciel existant ou installé sur l'appareil doit avoir été acquis légalement et être utilisé sous licence. En outre, il doit être installé conformément aux conditions de licence et d'utilisation. Ce principe s'applique aussi bien aux logiciels privés qu'aux logiciels mis à disposition par la BFH.
- *d* L'appareil doit être sécurisé au moyen de mesures de protection, à savoir un logiciel antivirus, une protection contre les malware, un Firewall local et une configuration adaptée. Si le système d'exploitation de l'appareil contient une fonction de cryptage de la mémoire de données, celle-ci doit être utilisée et configurée selon l'état de la technique.
- *e* L'utilisateur ou l'utilisatrice contribue de manière active à la résolution d'incidents informatiques survenant dans son activité ou impliquant son appareil.

[4] Les IT-Services offrent un support dans la mesure de leurs possibilités pour les appareils privés ou auto-administrés. Toutefois, aucun support n'est dû pour ce type d'appareil.

[5] L'utilisation d'un appareil privé ou auto-administré se fait à ses propres risques, la BFH déclinant toute responsabilité.

[6] Lorsqu'une personne utilisant un appareil privé ou auto-administré le remet à des tiers (p. ex. élimination, vente, réparation, etc.) ou qu'elle quitte la BFH, il lui incombe d'entreprendre préalablement les actions suivantes :

- *a* Remettre à la BFH toutes les informations appartenant à celle-ci et utilisées sur l'appareil.
- *b* Supprimer définitivement de l'appareil toutes les informations relatives à l'institution.
- *c* Désinstaller tous les logiciels pour lesquels la transmissibilité n'est pas explicitement mentionnée dans les conditions de licence.

3 Responsabilités (y compris responsabilité civile)

Art. 6 Respect du droit

[1] Chaque utilisateur et utilisatrice se conforme en tout temps aux lois et aux règlements actuels en vigueur, particulièrement en matière de protection des données et de droits d'auteur[2].

[2] Avant d'utiliser des ressources informatiques, en particulier des logiciels, l'utilisateur ou utilisatrice s'informe sur les conditions de licence valables et les respecte.

[3] Le traitement de données personnelles n'est autorisé que dans le cadre de travaux liés à la BFH respectant les dispositions sur la protection des données, en particulier la Loi sur la protection des données (LCPD)[3] et l'Ordonnance sur la protection des données (OPD)[4] qui en dérive.

Art. 7 Abus

[1] Est considérée comme abusive toute utilisation des ressources informatiques de la BFH qui contrevient aux prescriptions de ce règlement, au droit supérieur ou aux droits des tiers. Entrent notamment dans cette catégorie, à moins d'une autorisation exceptionnelle selon l'art. 3, al. 4 de cette directive, les utilisations suivantes :

- *a* Le traitement d'informations au contenu illégal ou indécent, en particulier les représentations de violence, la pornographie, l'incitation au crime ou à la violence, l'atteinte à la liberté religieuse ainsi que la discrimination raciale.
- *b* La production de programmes ou sous-programmes nuisibles (p. ex. virus, vers, chevaux de Troie, etc.), leur diffusion délibérée ou les conseils en vue de leur fabrication.
- *c* L'intrusion illicite dans un système de traitement de données dans ou hors de la BFH (hacking), notamment l'espionnage de mots de passe, la recherche -sans autorisation des IT-Services - des points faibles de réseaux internes ou externes à la BFH ainsi que des services informatiques (p. ex. balayage des ports), les mesures et exécutions de mesures visant à perturber des réseaux et services informatiques (p. ex. denial of service attacks).
- *d* Le vol ainsi que le traitement illégal d'informations, en particulier le fait de les copier, de les modifier ou de les supprimer.
- *e* La mise à disposition de contenus sur des services informatiques internes ou externes à la BFH, lorsque cette action constitue une violation de la législation en vigueur ou une menace pour l'image de la BFH. Il est notamment interdit de propager du matériel protégé par des droits d'auteur.
- *f* L'utilisation de moyens informatiques de la BFH en violation intentionnelle des conditions de licence ou des droits d'auteur.
- *g* L'acquisition, la sauvegarde, l'installation, l'activation ou l'utilisation de logiciels, de licences ou de services obtenus illégalement.
- *h* L'envoi de messages contenant des indications usurpées ou trompeuses d'expéditeur (y compris l'adresse technique) ou l'envoi indu d'e-mails de masse (p. ex. spams).
- *i* Le harcèlement ou la mystification de membres de la BFH ou de tiers par le biais de ressources informatiques (p. ex. e-mails au contenu offensant ou discriminatoire).
- *j* L'extension ou la modification de composants de réseau de la BFH (p.ex. modem, WLAN, Access Points).
- *k* L'utilisation de ressources informatiques pour calculer les moyens de paiement numériques, tels que Bitcoin.
- *l* L'utilisation de ressources informatiques dans le cadre privé dans un but commercial (par exemple SpinOff)

[2] RS 231.1.
[3] RSB 152.04.
[4] ORSB 152.040.1.

Art. 8 Conséquences en cas d'abus

[1] Tous les utilisateurs et utilisatrices sont directement et personnellement responsables de se conformer à cette directive ou au droit supérieur lors de l'utilisation des ressources informatiques et notamment de leur compte utilisateur BFH.

[2] Dans le cas où un abus des ressources informatiques est constaté ou soupçonné, les IT-Services peuvent prendre toutes les mesures nécessaires au rétablissement d'une situation conforme, à savoir :

- *a* Restreindre préventivement l'accès aux ressources informatiques concernées.
- *b* Saisir les informations abusives, les sauvegarder ou stocker comme preuves.
- *c* Supprimer des informations abusives, si cela s'impose pour des raisons de sécurité.
- *d* De telles mesures étant prises, avertir les responsables hiérarchiques des personnes contrevenantes.

[3] En cas d'abus, des sanctions peuvent être infligées aux utilisateurs et utilisatrices contrevenants, en vertu des règlements concernant le personnel ou les études.

[4] Sont réservées les poursuites pénales et les actions de nature civile.

Art. 9 Protection des données

[1] Pour garantir l'application de cette directive, des contrôles de plausibilité (échantillons) anonymes peuvent être effectués par les personnes chargées de la sécurité informatique, en collaboration avec les personnes responsables concernées.

[2] Pour garantir le fonctionnement des services informatiques, les données de protocole sont évaluées en cas de dérangement ou en vue de vérifier les fonctions techniques.

[3] Si une utilisation abusive des ressources informatiques est soupçonnée, la direction des IT-Services requiert auprès du recteur ou de la rectrice la mise en œuvre d'un contrôle annoncé, limité dans la durée et restreint à un cercle de personnes défini.

[4] Des activités réalisées en utilisant les ressources informatiques peuvent être enregistrées. Les données secondaires qui en résultent sont stockées, servant à tracer les fonctions techniques et à mettre les preuves en sécurité.

[5] Pour autant qu'elle soit applicable, l'Ordonnance sur les données secondaires de communication (ODSC)[5], est également valable pour l'accès aux données personnelles qui sont enregistrées lors de l'utilisation de l'infrastructure électronique (données secondaires) et pour leur évaluation.

[6] Les données secondaires contenant des données personnelles sont conservées pendant une période minimale de 6 mois et maximale d'un an. Une durée de conservation différente est autorisée si des dispositions légales ou règlementaires, notamment l'Ordonnance sur les données secondaires de communication, ou si cela est nécessaire à des fins de preuve. Une période transitoire jusqu'au 31.12.2021 s'applique pour la mise en œuvre.

Art. 10 Exclusion de la responsabilité

La BFH n'est pas responsable des dommages survenant lors de l'utilisation de moyens informatiques ou occasionnés par des moyens informatiques défectueux.

4. Dispositions finales

Art. 11 Dispositions finales

[1] Certains articles de cette directive peuvent être complétés par des annexes. Ces dernières doivent être validées par le recteur ou la rectrice.

[5] RSB 153.011.5.

[2] La présente directive remplace la version du 13 juillet 2016 portant sur l'utilisation des ressources informatiques à la Haute école spécialisée bernoise. Elle entre en vigueur à compter du 1er janvier 2021.

Berne, le 1er janvier 2021

Haute école spécialisée bernoise

Prof. Dr. Sebastian Wörwag
Recteur