Acceptable Use Policy

(La version française suit.)

1. The use of the DLN 3.0 is limited to authorized users – Learners and Administrators including DND employees, CAF members, contractors and other persons authorized to use the system only and is subject to the DND and CAF Code of Values and Ethics, the National Defence Security Orders and Directives (NDSODs) and applicable Defence Administrative Orders and Directives (DAODs). Users understand that any violation of the spirit or intent of these rules and regulations can lead to administrative or disciplinary action.
2. Authorized users may access the system using:
    a. A DWAN workstation at DND locations across the country;
    b. Remote access to the system through DVPNI;
    c. A personal device using either an HTML web browser or the Saba Cloud mobile app for iOS and Android devices.
3. Authorized users are prohibited from:
    a. Disclosing or sharing account credentials (username and password);
    b. Allowing unauthorized persons access to the system resources;
    c. Introducing any information to the system for which all other users are not cleared to access.
4. There shall be no expectation of privacy when using DLN 3.0. Users are subject to monitoring for the purposes of system administration, maintenance and security, and to ensure compliance with Treasury Board, DND and CAF policies, instructions, directives and standards.
5. DND/CAF information shall not be copied, or otherwise transferred from the DLN 3.0 environment to personal devices outside the associated internet browser session or approved DLN applications.
6. Downloading DND/CAF material deemed protected is not authorized on a personal device and can only be accessed within the confines of the browser session.
7. DND/CAF protected material that needs to be extracted from the system will need to be processed via a department approved DWAN device.

8. DLN 3.0 is only authorized for processing, and transmission of information up to and including Protected B (PB). The processing, storage, and transmission of Controlled Goods information and Data is not permitted in the application.
9. DND/CAF is not responsible for support to personal devices. Users assume responsibility for risks to personal devices, including but not limited to, partial or complete loss of data due to operating system crashes, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render devices unusable.
10. Although security features have been enabled to limit the risk to information and devices connecting to DLN 3.0, users are expected to remain alert to potential threats such as unsolicited emails, file attachments, and external links accessed via the DLN environment.
11. Should a risk to the DLN 3.0 or the information contained be detected and originating from a personal device (due to malware compromise or missing security updates for examples), the DLN team reserve the right to disable the associated account without notice.
12. The DLN 3.0 is operating under an interim authority to operate (iATO). Should any action from an account risk the integrity or security of the application, the DLN team reserve the right to disable the associated account without notice.

Terms and Conditions (Cornerstone) | Privacy (Cornerstone)

Politique d’utilisation

1. L’utilisation du Réseau d’apprentissage de la défense 3.0 (RAD 3.0) est limitée aux utilisateurs autorisés (apprenants, admirateurs incluant les employés du MDN, les membres des FAC, agents contractuels et autres personnes autorisées à utiliser le système. Tous les utilisateurs sont de plus assujettis aux codes d éthiques et de valeurs du MDN/FAC, les ordres de sécurités de la défense nationale et les Directives et Ordonnances Administratives de la Défense (DOAD) et Ordonnances et Directives de Sécurité de la Défense Nationale (ODSDN). Les usagers doivent comprendre que toute contravention à ces ordres, code et politiques peut mener à des mesures disciplinaires ou administratives.
2. Les usagers autorises peuvent accédé au système en utilisant:
    a. Un ordinateur du RED a partir d’un site du MDN/FAC;
    b. Un ordinateur du RED par l’entremise d’une connexion DVPNI;
    c. Un appareil personnel par l’entremise d’un navigateur web ou bien de l’application mobile Saba Cloud (iOS ou Android).
3. Les utilisateurs n’ont pas le droit de :
    a. Divulguer ou partager leur identifiants (nom d’utilisateur et mot de passe);
    b. Permettre des personnes non autorisées d’utiliser le système ou ses ressources;
    c. Introduire de l’information pour laquelle les autres usagers du système ne sont pas autorisés.
4. Les utilisateurs du RAD 3.0 doivent être conscients que le système est sujet à la surveillance pour les besoin de l’administration du système, sa maintenance, sa sécurité et le respect des politiques et directives du Conseil du Trésor, MDN at FAC.
5. L’information du MDN/FAC ne doit pas être copiée ou autrement transférée depuis l’environnement RAD 3.0 à un appareil personnel à part une session de navigateur web ou une application autorisée pour DLN 3.0.
6. Les téléchargements de contenus du MDN/FAC considérés PROTÉGÉ sont non-autorisés sur les appareils personnels et ces contenus doivent seulement être utilisés par l’entremise d’une session de navigateur.
7. L’information PROTÉGÉ qui doit être extraite du système RAD 3.0 devra

8. Le RAD 3.0 est autorisé seulement pout l'entreposage, traitement et transmission de l'information jusqu'à Protégé B (PB). L'entreposage, traitement ou transmission de contenus considérés Marchandises Contrôlées est interdite.
9. Le MDN ou les FAC sont non responsables pour supporter les appareils personnels incluant mais non restreint aux pertes de données occasionnes par les erreurs, virus, logiciel malveillant et les défauts de logiciel ou matériel, ou erreur de programmation qui pourraient rendre un appareil inutilisable.
10. Malgré que des contrôles de sécurité ont été mis en œuvre afin de minimiser les risques pour l'information et l'infrastructure du RAD, les utilisateurs sont tenus de rester vigilants vis-à-vis des menaces potentielles tels que les courriels non-sollicités ou les pièces-jointes ainsi que les liens externes accédés depuis le RAD.
11. Si un risque pour le RAD 3.0 ou son information est déterminé de provenir d'un appareil personnel (à cause d'un logiciel malveillant ou d'une carence de mises-à-jour de sécurité par exemple), l'équipe de support RAD 3.0 se réserve le droit de désactivé le compte d'utilisateur sans préavis.
12. RAD 3.0 opère en vertu d'une autorisation de sécurité intérimaire. Si des actions ou transactions risquant la sécurité du système ou de son information sont déterminées de provenir d'un compte d'utilisateur, l'équipe de soutien du RAD se réserve le droit d'inactiver le compte d'utilisateur en question.

Avis (Cornerstone) | Confidentialité (Cornerstone)