- documentation de processus d'escalade pouvant inclure des plans d'intervention en cas d'*incident de cybersécurité* prévus dans la norme CIP-008.

E2. Chaque entité responsable doit mettre en œuvre, sauf en cas de *circonstance CIP exceptionnelle*, un ou des processus documentés en vue de conserver les données de surveillance de sécurité de réseau interne associées à une activité réseau jugée anormale par l'entité responsable, au moins jusqu'à ce que les mesures pertinentes prévues à l'alinéa 1.3 de l'exigence E1 aient été prises.
[Facteur de risque de non-conformité : faible] [Horizon : exploitation le même jour et évaluation des activités d'exploitation]

Remarque : L'entité responsable n'est pas tenue de conserver des données de surveillance de sécurité de réseau interne qui ne sont pas pertinentes à une activité réseau anormale détectée selon l'alinéa 1.2 de l'exigence E1.

M2. Exemples non limitatifs de pièces justificatives : documentation du ou des processus de conservation des données de la surveillance de sécurité de réseau interne, configurations de systèmes ou rapports générés automatiquement attestant la conservation des données sur des périodes suffisantes pour la conformité à l'alinéa 1.3 de l'exigence E1.

E3. Chaque entité responsable doit mettre en œuvre, sauf en cas de *circonstance CIP exceptionnelle*, un ou des processus documentés visant à protéger les données de surveillance de sécurité de réseau interne collectées aux fins de l'exigence E1, ainsi que les données conservées aux fins de l'exigence E2, contre les risques de modification ou de suppression non autorisée.
[Facteur de risque de non-conformité : faible] [Horizon : exploitation le même jour et évaluation des activités d'exploitation]

M3. Exemples non limitatifs de pièces justificatives : documentation indiquant comment les données de surveillance de sécurité de réseau interne sont protégées contre les risques de modification ou de suppression non autorisée.

C. Conformité

1. Processus de surveillance de la conformité

1.1. Responsable des mesures pour assurer la conformité : Le terme « *responsable des mesures pour assurer la conformité* » (*CEA*) désigne la NERC ou l'*entité régionale*, ou toute entité désignée par un organisme gouvernemental pertinent, dans leurs rôles respectifs visant à surveiller et à assurer la conformité avec les *normes de fiabilité* obligatoires et exécutoires dans leurs territoires respectifs.

1.2. Conservation des pièces justificatives : Les périodes de conservation des pièces justificatives indiquées ci-après établissent la durée pendant laquelle une entité est tenue de conserver certaines pièces justificatives afin de démontrer sa conformité. Dans les cas où la période de conservation des pièces justificatives indiquée est plus courte que le temps écoulé depuis le dernier audit, le *CEA* peut demander à l'entité de fournir d'autres pièces justificatives attestant sa conformité pendant la période complète écoulée depuis le dernier audit.

L'entité responsable doit conserver les données ou les pièces justificatives attestant sa conformité selon les modalités indiquées ci-après, à moins que son *CEA* lui demande de conserver certaines pièces justificatives plus longtemps dans le cadre d'une enquête :

Ex.	Niveaux de gravité de la non-conformité			
	VSL faible	VSL modéré	VSL élevé	VSL critique
E2	S. O.	S. O.	S. O.	L'entité responsable n'a pas mis en œuvre, sauf en cas de *circonstance CIP exceptionnelle*, un ou des processus documentés en vue de conserver les données de surveillance de sécurité de réseau interne associées à une activité réseau jugée anormale par l'entité responsable, au moins jusqu'à ce que les mesures pertinentes prévues à l'alinéa 1.3 de l'exigence E1 aient été prises.
E3	S. O.	S. O.	S. O.	L'entité responsable n'a pas mis en œuvre, sauf en cas de *circonstance CIP exceptionnelle*, un ou des processus documentés visant à protéger les données de surveillance de sécurité de réseau interne collectées aux fins de l'exigence E1, ainsi que les données conservées aux fins de l'exigence E2, contre les risques de modification ou de suppression non autorisée.

D. Différences régionales

Aucune

E. Documents connexes

Lien vers le plan de mise en œuvre et d'autres documents connexes importants.

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	9 mai 2024	Approbation par le Conseil d'administration de la NERC.	
1	26 juin 2025	Ordonnance de la FERC approuvant la norme CIP-015-1. Dossier RD24-7-000.	