Shape

Description automatically generatedText

Description automatically generated with low confidence

|  |
| --- |
| Sylvain Depasse  [Date] |

|  |
| --- |
| Annex RAA1 |
| Revue Après Action |
| IRP RAA1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **CYBERSECURITE** | | |
| **POLITIQUE** | **Revue Après Action** | | | |
| **Policy ID:** | **Add ID Number** | **Date de création: 8/24/2022** | | |
| **Approved by:** |  | **Reviewed**  **(No changes made)** | **☐** | **Date** |
| **Approved by:** |  | **Revised**  **(Changes made)** | **☐** | **Date** |
| **Area:** | **Choose Area** | **Repealed**  **(No longer active)** | **☐** | **Date** |
| **Department:** | **Choose Department** | **Prior Policy: N/A** | | |
| **Applies to:** | **All Areas** |  | | |
|  | | | | |
| **Additional Approvals**  Additional reviews and approvals by internal and external stakeholders. | | | | |
| **Approver Title** | | **Area / State / Agency** | | |
|  | |  | | |
|  | |  | | |
|  | | | | |
| **Data Classification:** **Confidential** | | **Electronic Approvals are maintained in the Policy Repository** | | |
|  | | | | |
| **Additional Information:** | | | | |
|  | | | | |
|  | | | | |

Contents

[1 Introduction 3](#_Toc112236110)

[2 Définitions 3](#_Toc112236111)

[2.1 3](#_Toc112236112)

[3 Politique 3](#_Toc112236113)

[3.1 3](#_Toc112236114)

[4 References to Regulatory and Industry Standards 4](#_Toc112236115)

[5 References to Other Documents 4](#_Toc112236116)

[6 External References 4](#_Toc112236117)

# Introduction :

Ce document fait suite en complément au Respons Incident Plan

Il est supposé vous aider lors de la revue de l’incident, à vous poser les bonnes questions afin de tirer les meilleurs apprentissages possibles des incidents passés.

# Comment ?

Lors d’une réunion, réunissant les membres du personnel concernés et les clients concernés si tel est le cas.  
Cette réunion aura pour but d’être constructive, nous devrons donc y participer activement afin d’améliorer les process établit.   
N’hésitez donc pas à relever les points positifs que vous aurez notez, mais aussi les points négatifs quel qu’ils soient.

# Que doit-on revoir ?

Voici quelques questions intéressantes à se poser lorsque l’on veut tirer profit de l’expérience vécue :

1. Qu’est-ce qui s’est bien passé pendant l’enquête ?
2. Quelles choses ne se sont pas bien passées pendant l’incident ?
3. Quelles vulnérabilités ou lacunes dans l’état de sécurité de l’organisation ont été identifiés ?
   1. Comment les résoudre ?
   2. Si pas de résolution, comment les rendre inoffensifs ?
4. Quelles autres étapes ou actions auraient été utiles pour prévenir l’incident ?
5. Des modifications doivent-elles être apportées à l’un des éléments concernés ?  
    Exemples :
   1. Compromised credentials :
      1. Authentification multifacteur ?
      2. Revoir politique de MDP ?
   2. Segmentation du réseau ?
   3. Configuration firewall ?
   4. Procédures de mis à jour
   5. Formation des employés ? (Client, communication, CERT,..)

Les réponses à ces questions devraient déjà apporter une approche des améliorations possibles.

A la fin de cette réunion, un rapport technique de celle-ci devra être rédigée pour l’équipe CERT, ainsi qu’un résumé analytique qui devra être présenté à l’équipe de direction

# 

# Références aux Régulation et Standards

Les références aux standards internationaux et régulation relatives au secteur de l’entreprise sont repris dans le tableau ci-dessous.

|  |  |  |
| --- | --- | --- |
| **ISO 27001:2013** | **NIST SP 800-53** | **HIPAA** |
| A.8.1.3 Acceptable Use of Assets | AC-20, PL‑4, PS-6 | Workstation Use §164.310(b) |

# Références aux autres documents internes

Les références à d’autres politiques, standards, procédures ou documents internes sont listées dans le tableau ci-dessous.

|  |  |
| --- | --- |
| **Document Name** | **Document ID** |
| Non-discrimination and Anti-harassment Policy |  |

# Autres références externes

Les références utilisées ou citées durant la rédaction de ce document sont listées dans le tableau ci-dessous.

|  |  |  |  |
| --- | --- | --- | --- |
| **Référence** | **Titre** | **ID de Référence** | **Année** |
|  |  |  |  |