Envoyé en préfecture le 27/09/2024
Reçu en préfecture le 27/09/2024
Publié en ligne le 30/09/2024
ID : 040-244000865-20240926-20240926D09-DE

MACS
Communauté de communes
Maremne Adour Côte-Sud

COMMUNAUTÉ DE COMMUNES MAREMNE ADOUR CÔTE-SUD
SÉANCE DU 26 SEPTEMBRE 2024 À 18 HEURES 30
SALLE DU CONSEIL DU SIÈGE DE MACS À SAINT-VINCENT DE TYROSSE

Nombre de conseillers :
en exercice : 57
présents : 36
absents représentés : 13
absents excusés : 8

CONSEIL COMMUNAUTAIRE
SÉANCE DU 26 SEPTEMBRE 2024

L'an deux mille vingt-quatre, le vingt-six du mois de septembre à 18 heures 30, le conseil communautaire de la Communauté de communes Maremne Adour Côte-Sud, dûment convoqué le 18 septembre 2024, s'est réuni en session ordinaire, à la salle du conseil du siège de MACS à Saint-Vincent de Tyrosse, sous la présidence de Monsieur Pierre FROUSTEY.

Présents :
Mesdames et Messieurs Jean-Luc ASCHARD, Alexandrine AZPEITIA, Armelle BARBE, Jacqueline BENOIT-DELBAST, Emmanuelle BRESSOUD, Géraldine CAYLA, Frédérique CHARPENEL, Nathalie DARDY, Jean-Claude DAULOUÈDE, Sylvie DE ARTECHE, Bertrand DESCLAUX, Gilles DOR, Maëlle DUBOSC-PAYSAN, Régis DUBUS, Florence DUPOND, Pierre FROUSTEY, Louis GALDOS, Régis GELEZ, Olivier GOYENECHE, Patrick LACLÉDÈRE, Pierre LAFFITTE, Cédric LARRIEU, Marie-Thérèse LIBIER, Isabelle MAINPIN, Aline MARCHAND, Élisabeth MARTINE, Jean-François MONET, Stéphanie MORA-DAUGAREIL, Damien NICOLAS, Pierre PECASTAINGS, Kelly PERON, Philippe SARDELUC, Alain SOUMAT, Serge VIAROUGE, Christophe VIGNAUD, Mickaël WALLYN.

Absents représentés :
Mme Françoise AGIER a donné pouvoir à M. Jean-Luc ASCHARD, M. Henri ARBEILLE a donné pouvoir à M. Gilles DOR, M. Patrick BENOIST a donné pouvoir à Mme Aline MARCHAND, M. Francis BETBEDER a donné pouvoir à M. Régis GELEZ, M. Hervé BOUYRIE a donné pouvoir à M. Pierre FROUSTEY, M. Pascal CANTAU a donné pouvoir à Mme Sylvie DE ARTECHE, Mme Valérie CASTAING-TONNEAU a donné pouvoir à M. Pierre PECASTAINGS, M. Alain CAUNÈGRE a donné pouvoir à Mme Frédérique CHARPENEL, M. Benoît DARETS a donné pouvoir à Mme Nathalie DARDY, M. Jean-Luc DELPUECH a donné pouvoir à Mme Jacqueline BENOIT-DELBAST, M. Dominique DUHIEU a donné pouvoir à Mme Marie-Thérèse LIBIER, Mme Nathalie MEIRELES-ALLADIO a donné pouvoir à M. Patrick LACLÉDÈRE, M. Jérôme PETITJEAN a donné pouvoir à M. Olivier GOYENECHE.

Absents excusés : Mesdames Véronique BREVET, Séverine DUCAMP, Isabelle LABEYRIE, Messieurs Lionel CAMBLANNE, Mathieu DIRIBERRY, Eric LAHILLADE, Alexandre LAPÈGUE, Olivier PEANNE.

Secrétaire de séance : Madame Alexandrine AZPEITIA.

OBJET : NUMÉRIQUE - APPROBATION DE LA POLITIQUE DE SÉCURITÉ DES SYSTEMES D'INFORMATION DE MACS

Rapporteur : Madame Frédérique CHARPENEL

La Communauté de communes MACS a, entre autres, pour objectif d'offrir aux usagers du service public des services performants, de qualité et accessibles. Dans le cadre de ces missions, elle utilise des services informatiques et numériques et détient des informations de nature sensible.

Envoyé en préfecture le 27/09/2024
Reçu en préfecture le 27/09/2024
Publié en ligne le 30/09/2024
ID : 040-244000865-20240926-20240926D09-DE

Dans un monde où la cybermalveillance ne cesse de croître, la sécurité des acteurs et usagers de MACS et de ses systèmes d'information et outils numériques est devenue un enjeu stratégique. Défendre la Communauté de communes MACS contre les cybermenaces est une responsabilité partagée des élus, de la direction et des employés pour éviter les pertes financières et de réputation, ainsi que pour protéger les données sensibles et celles des administrés.

C'est pour cela qu'il est proposé au conseil communautaire d'approuver une politique de sécurité des systèmes d'information (PSSI) de MACS. Cette dernière se veut claire, pertinente et adaptée aux besoins de la Communauté de communes. Elle doit être communiquée à tous les acteurs pour les sensibiliser à l'importance de la sécurité des systèmes d'information ainsi qu'aux conséquences de leur comportement.

Cela implique des mesures opérationnelles et techniques, mais aussi organisationnelles comme la mise en place d'un plan de gestion de crise pour faire face aux éventuelles attaques ou incidents de sécurité.

Outre ces éléments, la Communauté de communes s'organise afin de se doter d'équipes et de compétences en charge de la mise en place et du maintien de la politique de sécurité et de la sécurité du système d'information.

La présente PSSI énonce l'intention de la Communauté de communes d'identifier et de protéger ses informations critiques des menaces pouvant être issues de mouvements étatiques, du crime organisé, du terrorisme, des activités idéologiques ou de démarches individuelles et pouvant toucher les principes de sécurité suivant :

- **la confidentialité :** l'information ne doit être accessible qu'au personnel autorisé,
- **la disponibilité** : propriété d'accessibilité au moment voulu des données et des fonctions par les utilisateurs autorisés,
- **l'intégrité** : l'information ne doit pouvoir être modifiée que par le personnel autorisé,
- **la traçabilité :** l'accès et les tentatives d'accès à l'information doivent être tracés afin de garantir la non-répudiation des actions réalisées.

Il faut également distinguer :

- les attaques visant directement le système d'information : vol de données (et éventuellement les ressources supportant ces données), modification des données, déni de service…,
- les attaques visant les ressources informatiques : vol de ressources, détournement des ressources, altération des données, émission de malware…,
- les accidents : sinistres naturels, altération accidentelle des données ou ressources…

Pour chaque menace, il est alors nécessaire d'en évaluer le risque, de considérer la probabilité que celle-ci devienne réalité et détecter les éventuels facteurs aggravants (négligence constatée, insuffisance d'information, de consignes…).

La PSSI s'applique à tous les utilisateurs ou bénéficiaires des ressources d'information de la Communauté de communes. S'ajoutent au champ d'application du document tous les consultants, prestataires, fournisseurs ou organismes appelés à accéder ou à utiliser le système d'information. La responsabilité de protéger les ressources incombe à tous les employés.

Cette politique couvre tous les systèmes d'information exploités par la Communauté de communes ou contractés auprès d'un tiers. Le terme Systèmes d'Information, définit l'environnement global et comprend, sans toutefois s'y limiter, toute la documentation, les contrôles physiques et logiques, le personnel, le matériel (par exemple, les ordinateurs de bureau, les serveurs, les périphériques réseau et les périphériques sans fil), les logiciels et les informations.

Le document de PSSI est annexé à la présente et sera régulièrement actualisé afin d'accompagner les évolutions technologiques et les besoins du territoire.

Le CONSEIL COMMUNAUTAIRE,

VU le code général des collectivités territoriales ;

VU les statuts de la Communauté de communes Maremne Adour Côte-Sud, tels qu'annexés à l'arrêté préfectoral PR/DCPPAT/2024/n° 107 en date du 8 avril 2024 portant modification des statuts de la Communauté de communes ;

VU les délibérations du conseil communautaire en date des 17 décembre 2015, 27 septembre 2016, 2 mai 2017, 6 décembre 2018, 26 novembre 2020, 25 mars 2021, 25 novembre 2021 et 28 mars 2024, portant définition et modifications de l'intérêt communautaire des compétences de MACS qui y sont soumises ;

Envoyé en préfecture le 27/09/2024
Reçu en préfecture le 27/09/2024
Publié en ligne le 30/09/2024
ID : 040-244000865-20240926-20240926D09-DE

VU le projet de politique de sécurité des systèmes d'information de MACS, ci-annexé ;

décide, après en avoir délibéré, et à l'unanimité,

- d'approuver le projet de politique de sécurité des Systèmes d'Information de la Communauté de communes, tel qu'annexé à la présente,
- d'autoriser Monsieur le Président ou son représentant à prendre tout acte et à signer tout document se rapportant à l'exécution de la présente.

La présente délibération pourra faire l'objet d'un recours contentieux pour excès de pouvoir dans un délai de deux mois devant le Tribunal administratif de Pau à compter de sa publication et de sa transmission au représentant de l'État dans le département. Outre l'envoi sur papier ou dépôt sur place, le Tribunal administratif de Pau pourra être saisi par requête déposée via le site www.telerecours.fr.

Fait et délibéré les jour, mois et an ci-dessus
Pour extrait certifié conforme
À Saint-Vincent de Tyrosse, le 26 septembre 2024

MAREMNE ADOUR CÔTE-SUD 40230

Le président,

Pierre Froustey

Envoyé en préfecture le 27/09/2024
Reçu en préfecture le 27/09/2024
Publié en ligne le 30/09/2024
ID : 040-244000865-20240926-20240926D09-DE

MAI 2024

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (PSSI)

MACS
Communauté de communes
Maremne Adour Côte-Sud

Envoyé en préfecture le 27/09/2024
Reçu en préfecture le 27/09/2024
Publié en ligne le 30/09/2024
ID : 040-244000865-20240926-20240926D09-DE

Suivi des modifications

Version	Date	Rédacteur	Nature de la modification	Autorité d'approbation

Classification - Diffusion

Classification	Diffusion
Public	Interne

TABLE DES MATIÈRES

Envoyé en préfecture le 27/09/2024
Reçu en préfecture le 27/09/2024
Publié en ligne le 30/09/2024
ID : 040-244000865-20240926-20240926D09-DE

1. Engagement de la direction

La communauté de communes MACS a, entre autres, pour objectif d'offrir aux usagers du service public des services performants, de qualité et accessibles. Dans le cadre de ces missions, La communauté de communes MACS utilise des services informatiques et numériques et détient des informations de nature sensible.

Dans un monde où la cybermalveillance ne cesse de croître, la sécurité des acteurs et usagers de la communauté de communes MACS et de ses systèmes d'informations et outils numériques est devenue un enjeu stratégique. Le présent document et les différents documents d'encadrement de la sécurité expriment cette vision de la communauté de communes MACS quant à cette importance stratégique de la sécurisation de son système d'information et de ses outils numériques.

Défendre la communauté de communes MACS contre les cybermenaces est une responsabilité partagée des élus, de la direction et des employés afin de protéger notre système d'informations pour éviter les pertes financières et de réputation, ainsi que pour protéger nos données sensibles et celles des administrés.

La communauté de communes MACS est résolument engagée dans cette démarche de sécurisation de nos actifs informationnels ce qui se traduit par différents éléments concrets.

Tout d'abord, nous avons demandé que soit élaborée la présente politique de sécurité des systèmes d'informations claire, pertinente et adaptée aux besoins de la Communauté de communes. Cette politique doit être communiquée à tous les acteurs pour les sensibiliser à l'importance de la sécurité des systèmes d'informations ainsi qu'aux conséquences de leur comportement sur la sécurité de la Communauté des communes.

De plus, nous veillerons à la mise en place de mesures de sécurité adéquates pour protéger les systèmes d'informations de la communauté de communes MACS. Cela implique des mesures de types opérationnelles et techniques, mais aussi un des mesures organisationnelles comme la mise en place d'un plan de gestion de crise pour faire face aux éventuelles attaques ou incidents de sécurité.

Outre ces éléments, la communauté de communes MACS s'organise afin de se doter d'équipes et de compétences en charge de la mise en place et du maintien de la politique de sécurité et de la sécurité du système d'information.

Parce que la sécurité des systèmes d'information et des outils numériques est l'affaire de tous, nous vous demandons de lui apporter tout votre concours.

Signature de l'organe de Direction

Prénom / Nom : .....

Qualité : .....

Signature

2. Contexte et enjeux

La communauté de communes MACS regroupe 23 communes :

- Angresse ;
- Azur ;
- Benesse-Maremne ;
- Capbreton ;
- Josse ;
- Labenne ;
- Magescq ;
- Messanges ;
- Moliets-et-Mâa ;
- Orx ;
- Saint-Geours-de-Maremne ;
- Saint-Jean-de-Marsacq ;
- Saint-Martin-de-Hinx ;
- Saint-Vincent-de-Tyrosse ;
- Sainte-Marie-de-Gosse ;
- Saubion ;
- Saubrigues ;
- Saubusse ;
- Seignosse ;
- Soorts-Hossegor ;
- Soustons ;
- Tosse ;
- Vieux-Boucau.

Du fait de l'interconnexion des services avec les différentes entités, la communauté de communes MACS a, notamment, pour objectifs de :

- Assurer aux acteurs qui gravitent autour de la communauté des communes la sécurité de leurs données, durant l'intégralité de leurs cycles de vie,
- Sensibiliser les usagers du territoire en rendant la sécurité de l'information accessible à tous,
- Cadrer la sécurité du système d'information de la communauté des communes de façon à respecter les règles à l'état de l'art, que ce soit en respectant les normes internationales de sécurité ou les bonnes pratiques édictées par les instances françaises et européennes en la matière,
- Harmoniser la sécurité des différentes entités composant ou utilisant le système d'information de la communauté de communes MACS afin de s'inscrire dans une démarche globale et efficiente,
- Permettre la résilience et la continuité des services informatiques de la communauté de communes MACS

2.1. Champ d'application

La politique de sécurité des Systèmes d'Information s'applique à tous les utilisateurs ou bénéficiaires des ressources d'informations de la Communauté de communes. S'ajoute au champ d'application du document tous les consultants, prestataires, fournisseurs ou organismes appelé à accéder ou à utiliser le système

d'information. La responsabilité de protéger les ressources incombe à tous les employés.

Cette politique couvre tous les systèmes d'information exploités par la Communauté de communes ou contractés auprès d'un tiers. Le terme Systèmes d'Informations, définit l'environnement global et comprend, sans toutefois s'y limiter, toute la documentation, les contrôles physiques et logiques, le personnel, le matériel (par exemple, les ordinateurs de bureau, les serveurs, les périphériques réseau et les périphériques sans fil), les logiciels et les informations.

Bien que cette politique couvre explicitement les responsabilités des utilisateurs, elle ne couvre pas exclusivement la question. D'autres politiques, normes, directives et procédures de sécurité définissent des responsabilités supplémentaires.

Tous les utilisateurs sont tenus de lire, de comprendre et de se conformer aux autres politiques, normes et procédures de sécurité de l'information selon la catégorie d'emploi qu'ils occupent et en lien direct avec celui-ci. Si un utilisateur ne comprend pas complètement quoi que ce soit dans ces documents, il doit contacter l'équipe en charge de la sécurité des Systèmes d'Information et l'équipe en charge des ressources humaines.

2.2. Besoins de sécurité

On désigne par sécurité de l'information l'ensemble des moyens techniques et non-techniques, permettant à un système numérique de résister à des événements (intentionnels ou non) susceptibles de compromettre la Disponibilité, l'Intégrité, la Confidentialité et la Traçabilité des données, traitées, stockées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles.

La présente politique énonce l'intention de la communauté de communes MACS d'identifier et de protéger ses informations critiques des menaces pouvant être issues de mouvement étatiques, du crime organisé, du terrorisme, des activités idéologiques, amateurs et pouvant toucher les principes de sécurité suivant :

- **La confidentialité :** L'information ne doit être accessible qu'au personnel autorisé.
- **La disponibilité** : Propriété d'accessibilité au moment voulu des données et des fonctionspar les utilisateurs autorisés.
- **L'intégrité** : L'information ne doit pouvoir être modifiée que par le personnel autorisé.
- **La traçabilité :** L'accès et les tentatives d'accès à l'information doivent être tracés afin de garantir la non-répudiation des actions réalisées.

On distingue ainsi :

- Les attaques visant directement le système d'information : vol de données (et éventuellement les ressources supportant ces données), modification des données, dénide service...
- Les attaques visant les ressources informatiques : vol de ressources, détournement des ressources, altération des données, émission de malware...
- Les accidents : sinistres naturels, altération accidentelle des données ou ressources... Pour chaque menace, il est alors nécessaire d'en évaluer le risque, i.e. considérer la probabilité que celle-ci devienne réalité et détecter les éventuels facteurs aggravants(négligence constatée, insuffisance d'information, de consignes...).

3. Mise en œuvre de la PSSI à la Communauté de communes Maremne-Adour Côte-Sud

La communauté de communes MACS met en œuvre une gouvernance de la sécurité des Systèmes d'Informations dont les exigences de sécurité suivent les règles édictées par les normes internationales ISO/IEC 27001 et ISO/IEC 27002.

Responsabilité des différents acteurs

Il est de la responsabilité de tous les employés de la Communauté de communes, des prestataires et sous-traitants ayant accès au Système d'Informations de se conformer à cette politique et aux autres politiques de sécurité associées. L'équipe de sécurité de l'information est responsable de l'examen et de la mise à jour de cette politique au besoin et/ou au moins une fois tous les 2 ans.

Au sein de la communauté de communes MACS, la responsabilité générale de la sécurité des systèmes d'information relève de la Direction des Systèmes d'Informations et du Numérique (DSIN) pour la Sécurité des Systèmes d'Information. Il est assisté dans cette fonction par le(la) Directeur(trice) des Systèmes d'Informations et du Numérique et par le(la) Responsable du pôle systèmes et Réseaux.
La PSSI de la communauté de communes MACS s'inscrit dans le cadre de la politique et des directives émanant de l'ANSSI (Agence National de la Sécurité des Systèmes d'Informations), en charge de la sécurité des systèmes d'information au niveau national.
Le pilotage courant est de la responsabilité de la DSIN et de son équipe.

La mise en œuvre opérationnelle est assurée par le(la) DSIN et son équipe pour le contrôle des données entrantes et sortantes ainsi que le service commun informatique et multimédia qui gère la chaine fonctionnelle des ressources institutionnelles.
Les responsables hiérarchiques de composantes (directeurs) sont responsables de la sécurité des systèmes d'information de leur périmètre

3.1. Dérogation

Il peut être nécessaire, dans certains cas, de déroger à des règles énoncées par la PSSI. Pour chacune de ces règles, la dérogation, motivée et justifiée, doit être expressément accordée par le DSI. La décision de dérogation, accompagnée de la justification, est tenue à la disposition de la DSI.

3.2. Organisation :

Responsable de la Sécurité des Systèmes d'Information

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) exerce sous l'autorité directe du (de la) DSIN, les activités suivantes :

- Contribuer activement à l'élaboration d'une politique de sécurité cohérente admise par tous et la mettre en œuvre,
- Viser tous les projets de l'établissement afin de veiller à la mise en œuvre au sein de ces derniers des éléments technologiques nécessaires à l'application de la PSSI,

- Faire connaître et respecter la charte d'utilisation des moyens informatiques et réseau de l'établissement.
- Proposer et mettre en œuvre des actions de sensibilisation et d'information de tous les utilisateurs aspects sécurité des systèmes d'information,
- Être l'intermédiaire direct en cas de problème entre la Communauté de communes et les acteurs compétentes.

Cette fonction est assurée par le (la) Directeur(trice) des Systèmes d'Informations et du Numérique.

Comité Cybersécurité

Le comité Cybersécurité se réunit tous les trimestres.

Les membres permanents sont :

- Directeur(trice) Général(e) des services ;
- Responsable du service juridique ;
- Directeur(trice) des Ressources Humaines ;
- Responsable du service Communication ;
- Directeur(trice) financier(e) ;
- Directeur(trice) des Systèmes d'Information et du Numérique.

3.3. Sécurité des Ressources Humaines

Charte informatique

Préalablement à son accès aux outils informatiques, l'utilisateur doit prendre connaissance des droits et devoirs que lui confère la mise à disposition par sa composante de ces outils. Cette information se fait au travers de la CHARTE D'UTILISATION des Moyens & Outils Technologiques de l'Information de la Communication (MOTIC) intégrée dans le règlement intérieur de la communauté de communes MACS.

Programme de sensibilisation à la sécurité

Il est important de mettre en œuvre des initiatives de sensibilisation à la sécurité à tous les niveaux de l'organisation, y compris les élus et tous les acteurs gravitant autour de la Communauté de communes.
D'une part, chaque nouvel employé bénéficie d'une sensibilisation à la sécurité des systèmes d'informations et d'autre part les séances de sensibilisation à la sécurité de l'information sont une initiative continue qui permet de s'assurer que tous les employés et intervenants sont au courant des politiques de sécurité de l'information qui les concernent.

3.4. Contrôle d'accès logique

La communauté de communes MACS ayant conscience du caractère critique de la gestion de ses solutions de contrôle d'accès logique, les éléments relatifs à la sécurité des accès logiques sont explicités dans les Directives associées.

3.5. Gestion des actifs

La communauté de communes MACS ayant conscience du caractère critique de la gestion de ses actifs les éléments relatifs à sa gestion sont explicités dans les Directives associées.

3.6. Sécurité physique et environnementale

La communauté de communes MACS ayant conscience du caractère critique de la sécurité des locaux, les éléments relatifs à la gestion de la sécurité physique et environnementale sont explicités dans les Directives associées.

3.7. Sécurité liée à l'exploitation

La communauté de communes MACS ayant conscience du caractère critique de la sécurité liée à l'exploitation des systèmes d'information, les éléments relatifs à la sécurité de l'exploitation sont explicités dans les Directives associées.

3.8. Sécurité des communications

La communauté de communes MACS ayant conscience du caractère critique de la sécurité liée aux communications, les éléments relatifs à la sécurité des communications sont explicités dans les Directives associées.

3.9. Acquisition, développement et maintenance des SI

La communauté de communes MACS ayant conscience du caractère critique de la sécurité liée au développement, les éléments relatifs à l'acquisition, le développement et la maintenance des SI sont explicités dans les Directives associées.

3.10. Relations avec les fournisseurs

La communauté de communes MACS ayant conscience du caractère critique de la sécurité liée aux fournisseurs, les éléments relatifs aux fournisseurs sont explicités dans les Directives associées.

3.11. Gestion des incidents liés à la SSI

La communauté de communes MACS ayant conscience du caractère critique du traitement des incidents de sécurité, les éléments relatifs à la gestion des incidents sécurité sont explicités dans les Directives associées.

3.12. Gestion de crise

La communauté de communes MACS ayant conscience du caractère critique de la gestion de crise, les éléments relatifs à la gestion de crise sont explicités dans les Directives associées.

3.13. Gestion de la continuité de l'activité

La communauté de communes MACS ayant conscience du caractère critique de la continuité de l'activité, les éléments relatifs à la sont explicités dans les Directives associées.

3.14. Conformité

La communauté de communes MACS ayant conscience du caractère critique de la conformité, les éléments relatifs à la conformité sont explicités dans les Directives associées.

3.15. Suivi, mesure, analyse et évaluation

La communauté de communes MACS ayant conscience du caractère critique du suivi de la sécurité de l'information, les éléments relatifs à la mesure et à l'évaluation de la sécurité de l'information sont explicités dans les Directives associées.

4. Amélioration continue

La politique d'amélioration continue de la communauté de communes MACS consiste à :

- Améliorer continuellement l'efficacité de la gestion de la sécurité des systèmes d'information,
- Améliorer les processus actuels pour les mettre en conformité avec les bonnes pratiques telles que définies par ISO/IEC 27001 et les normes connexes,

- Augmenter le niveau de proactivité en matière de sécurité de l'information,
- Rendre les processus et les contrôles de sécurité de l'information plus mesurables afin de fournir une base solide pour des décisions éclairées,
- Examiner périodiquement les paramètres pertinents pour déterminer s'il est approprié de les modifier, en fonction des données historiques collectées,
- Examiner les idées d'amélioration lors des réunions régulières du comité de suivi de la SSI.

5. Respect des exigences légales et contractuelles

La communauté de communes MACS doit protéger ses informations sensibles contre toute divulgation non autorisée. Les principales lois et réglementations de référence sont les suivantes :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)[1]

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004-801 du 6 août 2004 et par la loi n° 2018-493 du 20 juin 2018

Dispositions Pénales :
-Code Pénal (partie législative) : art 226-16 à 226-24
-Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13

Loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain.
Dispositions pénales : art 323-1 à 323-7 du Code pénal.

Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels.
Disposition pénale : art L.335-2 du Code pénal.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)

Loi n°2009-1311 relative à la protection pénale de la propriété littéraire et artistique sur internet dite HADOPI 2

Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure dite LOPPSI 2 (pour le délit d'usurpation d'identité numérique)
Dispositions pénales : art 226-4-1 du Code pénal.

Référentiel général d'amélioration de l'accessibilité (RGAA v4.1.2) du 18 février 2021

Loi n° 84-53 du 26 janvier 1984 modifiée (art. 89 et 90) et le décret n° 89-677 du 18 septembre 1989 relatif à la procédure disciplinaire applicable aux fonctionnaires territoriaux.

[1] Le délégué à la protection des données (DPO) conseille et accompagne la communauté de communes MACS dans sa mise en conformité au RGPD.

Décret n° 92-1194 du 4 novembre 1992 (art. 6) fixant les dispositions communes applicables aux fonctionnaires, stagiaires de la fonction publique territoriale.

Décret n° 88-45 du 15 février 1988 (art. 36 et 37) relatif aux agents non titulaires.

Décret n 91-298 du 20 mars 1991 (art. 15) relatif aux agents à temps non complet.

Respect de la propriété intellectuelle

L'utilisation des ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits.
En conséquence, chaque utilisateur doit :

- Utiliser les logiciels dans les conditions des licences souscrites ;
- Ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

Respect du droit d'auteur :

Conformément à l'article défini par l'article L113-2 du Code de la Propriété Intellectuelle :
« Est dite collective l'œuvre créée sur l'initiative d'une personne physique ou morale qui l'édite, la publie et la divulgue sous sa direction et son nom et dans laquelle la contribution personnelle des divers auteurs participant à son élaboration se fond dans l'ensemble en vue duquel elle est conçue, sans qu'il soit possible d'attribuer à chacun d'eux un droit distinct sur l'ensemble réalisé. »
Il s'agit du cas où une œuvre est pilotée est dirigée par un employeur, et où les contributions des salariés forment un tout impossible à séparer.
Dans ce cas, l'employeur est considéré comme l'auteur dès lors qu'il a le rôle de maître d'œuvre, tel un chef d'orchestre.

6. Révision

La politique de sécurité de l'information de la Communauté de communes, ainsi que les autres politiques de sécurité, doivent être revues périodiquement.
Cet examen aura lieu dans les circonstances suivantes :

- Une fois tous les 24 mois,
- S'il y a un changement significatif dans les technologies utilisées par la Communauté de communes,
- S'il y a un changement important dans l'environnement de la menace externe, ce qui exige un examen du profil de risque,
- S'il y a un changement important dans la règlementation en matière de sécurité de l'information
-

7. Communication

- La politique d'information sera diffusée à tous les employés et intervenants par courrier électronique, ou disponible sur Intranet.
- Toutes les communications liées aux médias des parties prenantes et aux marchés financiers seront effectuées par l'équipe de direction uniquement en fonction des besoins lors d'événements de presse, de conférences, de courriels. Aucun employé de l'organisation jusqu'à ce qu'il soit autorisé par l'organe de Direction ne peut échanger d'information avec les médias ou les marchés financiers.
- Tous les employés dans leur travail quotidien, doivent fonctionner en tant que représentants et ambassadeurs de la Communauté des communes et sont autorisés à échanger avec les tiers en accord avec leurs projets et domaines de responsabilité. Les informations échangées sont tenues confidentielles.
- Les informations sur la Communauté des communes ne doivent être diffusées sur le web qu'après l'approbation de la Direction de la communication.
- La communication avec les intervenants internes et externes doit être conforme à la position et à la stratégie de l'organisation et se fera en fonction de l'appréciation de la Direction de la communication.

8. Sanctions

Les mesures disciplinaires nécessaires seront prises à l'encontre de tout employé ne respectant pas les politiques et procédures établies par la Communauté des communes. De même, des mesures seront prises contre les employés qui encouragent/observent une telle activité et ne la signalent pas à l'autorité concernée. Tout employé reconnu coupable d'avoir enfreint cette politique peut faire l'objet de mesures disciplinaires.

Envoyé en préfecture le 27/09/2024
Reçu en préfecture le 27/09/2024
Publié en ligne le 30/09/2024
ID : 040-244000865-20240926-20240926D09-DE

Un document conçu par la Direction des Systèmes d'Informations :
dsi@cc-macs.org

MACS
Communauté de communes
Maremne Adour Côte-Sud