NEXT ENGINE

情報セキュリティチェックシート

Hamee株式会社
お問い合わせ先：プラットフォーム事業推進部
最終更新日：2022年3月3日

Hamee株式会社では法令及びその他の規範を遵守し、情報セキュリティへの取り組みを行っております。
本チェックシートは当社並びに当社のサービスについてセキュリティ対策を記載したものです。
なお、記載事項は運用や改善のため変更する場合があります。

ネクストエンジン　セキュリティチェックシート			
	設問	回答	詳細
各種認証			
1	プライバシーマーク（JIS Q 15001）の認証を取得している	○	登録番号：第17000786号　　登録日：5/23/2011
情報セキュリティ			
2	従業者（社員等）が入社する際には、業務上知りえた機密情報、個人情報の秘密を保持する内容が記載された誓約書等を取得している	○	入社時に全従業員より秘密保持契約書を締結
3	経営陣によって承認された個人情報や機密情報の保護に関する考え方や方針に関する宣言を策定し、ホームページなどで外部に公表している	○	プライバシーポリシーURL：https://hamee.co.jp/privacy
4	不正アクセス防止策や個人情報保護管理者の設置、内部関係者の情報持ち出し防止措置の情報セキュリティの仕組み等を整備する体制がありその責任者が定められている	○	苦情及び相談窓口責任者　ICT推進部　マネージャー
5	セキュリティ事故発生時における連絡ルートが確立している	○	プラットフォーム事業推進部担当 → ご担当者様へ連絡
6	建物、オフィスフロア、業務作業スペースなど、入退室（館）管理が実施されている	○	IDカード認証による入室管理システムを導入
7	紙や電子データなどで提供されたデータやデータを格納していたハードウェアは適切な返却、消去、廃棄を行っている	○	・紙媒体 シュレッダーによる廃棄を実施 ・電子媒体（CD-R、USBメモリー等） 電子媒体は使用できない/適切に破棄を実施 ・電子データ（パソコンやサーバのデータ） 適切に破棄を実施 ・PCやサーバー等の機器の廃棄 適切に破棄を実施
8	コンピュータウィルスなど、悪意のあるソフトウェアからの保護対策として、全てのPCにウィルス対策ソフトをインストールしている	○	ウイルス定義ファイルの更新間隔：自動アップデート
9	悪意ある第三者や過失による事故から情報資産を保護するため、当社の情報システムを利用する際は、ID（アカウント）認証によって利用できるよう設定している	○	・ID（アカウント）は利用者が特定できるように利用者毎に個別のアカウントを発行 ・パスワードを一定回数、間違えるとアカウントを凍結する仕組みがある ・退職者ID（アカウント）は所管部署から速やかにシステム管理部署へ申請書を提出し、削除
10	不正アクセスや不正利用を検出し情報セキュリティレベルを維持管理する目的で、システムによるアクセス・ログなどの方法で機密データや個人情報データにアクセスした記録を作成し保持している	○	各種ログデータを取得し、定期的に確認
11	法令や他社との契約上の義務に違反がないかチェックしている	○	プライバシーマークに基づき、遵守状況を内部監査部門が監査
12	法令や他社との契約上の義務を担当者に説明している	○	ネクストエンジンの利用規約等が周知されている
13	個人情報や機密情報の持ち出しを禁止、又は制限している	○	・外部記憶媒体の利用をシステム的に制限 ・機密情報が保存された端末の持ち出しを禁止
14	雇用する従業者（派遣社員や委託スタッフを含む）に入社時以降、定期的に情報セキュリティ／個人情報保護に関する社内教育を行っている	○	週１回の全社アナウンスで教育を実施（１回／週）
15	情報セキュリティ／個人情報保護に関する定期的な監査（チェック）活動を行っている	○	内部監査部門が、年間を通して全部門の監査を実施（１回／年）
16	業務の再委託をする場合、委託先を適切に管理している	○	委託先に関し、定期的に委託先評価を行っている
個人情報保護			
17	個人情報保護法に基づき、個人情報を保護するための内部規程やマニュアル、入手、保管、廃棄など個人情報の管理に関する手順書などがある	○	
18	お客様、お取引先様、従業員などに対して個人情報の取得時には、本人へ利用目的を明確に伝えている	○	Webの登録フォームに個人情報保護方針や利用規約等のリンクを設置し、同意を得ている
19	個人情報の入手（取得）・保管・廃棄の各プロセスにおいて安全性に配慮している	○	・入手（取得）について メールやWebで受ける場合はパスワードを設定している/書類は追跡可能な方法で受渡ししている ・保管について 書類は施錠管理を実施/データはパスワード設定やアクセス権の制限がある ・廃棄について 紙媒体はシュレッダーによる廃棄/電子媒体は適切に破棄を実施
20	取得している個人情報の取り扱い状況を一覧できる手段がある	○	部門ごとに個人情報管理台帳を作成し、保管場所・保管方法・利用目的・アクセス権を有する者・利用期限等が分かるように管理している
21	個人情報を取り扱う情報システムは個人情報保護の配慮や運用の定期的な見直しをしている	○	定期的に棚卸し、アクセス権の見直しを実施している
22	お客様情報など個人情報を取り扱う作業エリアは特別な対策を行っている	○	・個人情報を扱う作業エリアはID毎の入退室管理を実施している執務エリアのみに作業エリアを限定している ・執務エリアは、IDカードによる入退出管理を行っている ・データへのアクセス権により担当者を限定しているが、物理的な制限はしていない