マジックシステム株式会社セキュリティポリシー

1. 目的

本ポリシーは、会社の開発環境およびその他の情報システム、データ、およびネットワークのセキュリティを確保し、不正アクセス、情報漏洩、データ破損、およびその他のセキュリティリスクを最小限に抑えることを目的とします。

2. 適用範囲

本ポリシーは、すべての従業員、契約社員、外部協力者、およびその他の関係者が使用する情報システム、ネットワーク、デバイスに適用されます。

3. 責任と役割

（1）情報セキュリティ責任者

セキュリティポリシーの実施と監督を行い、定期的にリスク評価を実施します。

（2）システム管理者

サーバー、ネットワーク機器、ソフトウェアの管理を担当し、システムのセキュリティ対策を実施します。

（3）従業員

個々の従業員は、セキュリティポリシーを遵守し、情報資産を適切に扱う責任があります。

4. データセキュリティ

（1）機密情報の取扱い

機密情報（顧客情報、従業員データ、企業機密など）は、アクセス制御が施された場所でのみ保管されるものとします。

（2）バックアップ

重要データは定期的にバックアップを取り、安全な場所に保管します。

（3）データアクセス権限の管理

各従業員に必要なデータアクセス権を付与し、職務変更に伴いアクセス権限の見直しを行います。

5. ネットワークセキュリティ

複数系統 LAN を置き、情報業務用のネットワークは強化されたセキュリティ対策が施されており、所定の機器しか使用しないこととし、不正なアクセスを防止します。

リモートワークを行う従業員は、必ず指定の LAN、ツールを使用し、社内ネットワークにアクセスするものとします。

6. 物理的セキュリティ

（1）施設へのアクセス管理

社内へのアクセスは、厳重に管理し、不要な人の出入りを制限します。

（2）デバイスの保護

ノートパソコンやモバイルデバイスは、常に鍵のかかる場所に保管し、外出時には必ず携帯して不正アクセスを防止します。

7. パスワード管理

（1）強固なパスワードの使用

全てのシステムにおいて、強力なパスワード（大文字、小文字、数字、特殊文字を含む）を使用し、定期的に変更します。

（2）パスワードの共有禁止

パスワードは他者と共有せず、定期的に変更します。

8. 教育と意識向上

（1）定期的なセキュリティ教育

全従業員は、情報セキュリティに関する定期的なトレーニングを実施します。

（2）フィッシング攻撃の対策

フィッシング攻撃の識別方法や対策について教育し、不審なメールの開封やリンクのクリックを避けるようにします。傾向の学習、教育を継続していきます。

9. インシデント対応

（1）セキュリティインシデントの報告

セキュリティインシデント（データ漏洩、マルウェア感染、システム障害など）を発見した場合、直ちに情報セキュリティ責任者に報告し、迅速に対応します。

（2）ウイルス対策ソフトウェア

全てのデバイスには最新のウイルス対策ソフトウェアをインストールし、定期的に更新します。

１０．懲戒処分

これらの規定を遵守しなかった役員、従業員には解雇を含む懲戒処分、賠償金を課すことがあります。

当セキュリティポリシーは公開するため、必須で守るべきルールを示したものであり、更なるセキュリティの管理方法や技術内容、監査方法については、セキュリティの確保のため、非公開とさせていただきます。

2024 年 11 月 29 日

マジックシステム株式会社

代表取締役社長 奥 兼範