

文書番号		セキュリティマニュアル	頁	1/8	
版 数	1		承認	承認	作成
制 定 日	2019 年 4 月 1 日				
改 訂 日	2019 年 4 月 1 日				
実施開始日	2019 年 4 月 1 日				

目次

1. 本書の目的	2
1-1. 目的	2
1-2. 対象者	2
2. 定義	2
3. 体制・役割	3
4. ICT 情報セキュリティ事務局の活動	5
4-1. ICT 使用およびリモート接続に関わる基準	5
4-2. ICT 情報セキュリティ活動計画	5
4-3. ICT 情報セキュリティ教育	5
4-4. ICT 情報セキュリティ自己点検	5
4-5. ICT 情報セキュリティ担当役員への報告	5
4-6. 基準文書の見直し	5
5. ITS の活動	6
5-1. 情報機器使用に関する基準	6
5-1-1. 申請の受理	6
5-2. システム使用許可に関する基準	6
5-2-1. ID の発行に関する基準	6
5-2-2. 特権 ID の発行に関する基準	6
5-2-3. 異動・退職時の ID の取扱	6
5-2-4. アクセス制限に関する基準	6
6. 例外事項	7
7. 罰則事項	7
改訂履歴表	8

文書番号		セキュリティマニュアル	頁	2/8
------	--	-------------	---	-----

1. 本書の目的

1-1. 目的

本文書は、ICT 情報セキュリティ事務局のセキュリティ推進活動および ITS のセキュリティに関わる統制活動の基準・規定に関する文書である。ICT 情報セキュリティ事務局が行う活動や情報機器やシステムの使用を許可する基準を明確化することを目的とする。

1-2. 対象者

ICT 情報セキュリティ事務局および ITS。

2. 定義

- (1) 「情報機器」とは、PC、モバイルデバイス、電子媒体の総称とする。
- (2) 「PC」とは、社内に設置された社内 LAN パソコン（仮想 PC も含む）、モバイル PC の総称とする。
- (3) 「モバイルデバイス」とは、以下「モバイル PC」と「スマートデバイス」の総称とする。
- (4) 「モバイル PC」とは、社外に持ち出し可能なパソコンをいう。
- (5) 「スマートデバイス」とは、スマートフォンやタブレット等、パソコンと異なり、キーボードを使わず指やタッチペンでタッチスクリーンを操作する端末をいう。
- (6) 「電子媒体」とは、USB メモリ等可搬型の大容量記録媒体をいう。
- (7) 「当社」とは、池田糖化グループをいう。
- (8) 「従業員等」とは、当社の役員及びこれに準じる者並びに従業員（嘱託、パートタイマー、アルバイト、派遣社員及び当社の関係会社からの受入者を含む。）をいう。
- (9) 「ITS」とは、アイティエス システム部門をいう。
- (10) 「ICT 情報セキュリティ事務局」とは、ICT 情報セキュリティ推進の事務を行う組織をいう。

文書番号		セキュリティマニュアル	頁	3/8
------	--	-------------	---	-----

3. 体制・役割

(1) ICT 情報セキュリティ担当役員

- ・ 代表取締役社長から任命され、池田糖化グループにおける ICT 情報セキュリティマネジメントに介しての最高責任者である。
- ・ ICT 使用およびリモート接続に関わる基準の運用、維持、継続的改善に責任を有し、率先して推進する。
- ・ ICT 情報セキュリティ委員会を統括し、必要な会議等を招集する。
- ・ 情報セキュリティ事故の報告を受けて、必要な対処を指示する。
- ・ ICT 情報セキュリティ事務局が策定した ICT 使用およびリモート接続に関わる基準を承認する。
- ・ 代表取締役社長ならびに役員に情報セキュリティ状況を報告する。

(2) ICT 情報セキュリティ推進責任者

- ・ 共通課題を抱える複数の組織の集合体（営業部門、開発部門など）や関連会社ごとに教育および点検作業等の ICT 情報セキュリティ施策を推進する。
- ・ ICT 情報セキュリティ事務局と連携して、組織外部での事故事例等を入手し、それらを所属の部門へ周知して注意喚起を図る。
- ・ 情報セキュリティ事故・違反を ICT 情報セキュリティ担当役員に報告する。

(3) ICT 情報セキュリティ推進担当者

- ・ ICT 情報セキュリティ推進責任者から各部門に最低一人は任命され、配置される者である。
- ・ 所属の従業員等に対し、普及・啓発を行う。
- ・ 情報セキュリティ事故・違反が発生した場合には、速やかに ICT 情報セキュリティ推進責任者に報告する。
- ・ ICT 使用およびリモート接続に関わる基準に対する意見や要望を収集し、ICT 情報セキュリティ事務局に報告する。
- ・ ICT 情報セキュリティ事務局と連携した上で、従業員等の教育および点検作業を支援、取りまとめを行う。

(4) ICT 情報セキュリティ委員会

- ・ 情報セキュリティを維持していくために、ICT 情報セキュリティ委員会を設け、全社的なマネジメント体制を整える。
- ・ ICT 情報セキュリティ担当役員、ICT 情報セキュリティ推進責任者、ICT 情報セキュリティ事務局で構成され、ICT 情報セキュリティ担当役員を委員長とする。
- ・ 不定期に開催し、ICT 使用およびリモート接続に関わる基準が周知されているか等活動状況と課題点を情報共有する。また、必要に応じて施策を協議する。

文書番号		セキュリティマニュアル	頁	4/8
------	--	-------------	---	-----

(5) ICT 情報セキュリティ事務局

- ・ ICT 情報セキュリティ担当役員の指示のもと、ICT 使用およびリモート接続に関わる基準を策定・改訂する。
- ・ ICT 使用およびリモート接続に関わる基準を配布し公開する。
- ・ ICT 使用およびリモート接続に関わる基準を基に、ICT 情報セキュリティマネジメント活動計画を作成する。
- ・ ICT 使用およびリモート接続に関わる基準を継続的に維持する。
- ・ 情報セキュリティ事故、違反等の例外事象を速やかに ICT 情報セキュリティ担当役員に報告すると共に対応を行い、必要に応じて対策を講じる。
- ・ ICT 情報セキュリティマネジメント活動計画にもとづき情報セキュリティ教育・点検を計画・実施し、結果を ICT 情報セキュリティ担当役員に報告する。
- ・ ICT 情報セキュリティ推進担当者から収集した情報を ICT 情報セキュリティ担当役員に報告する。

(6) ICT 情報セキュリティ運用管理者

- ・ ICT 情報セキュリティ事務局の管理のもとで、情報機器、システムのセキュリティ対策の責任を有する。
- ・ 各システム、情報機器の管理や、教育、点検の実施について、ICT 情報セキュリティ運用担当者を割り当てる。

(7) ICT 情報セキュリティ運用担当者

- ・ ICT 情報セキュリティ運用管理者の管理のもとで、教育・点検などの実質的な作業を行う。
- ・ 管理を依頼されたシステム、情報機器に対してセキュリティ対策を実施する。

文書番号		セキュリティマニュアル	頁	5/8
------	--	-------------	---	-----

4. ICT 情報セキュリティ事務局の活動

4-1. ICT 使用およびリモート接続に関わる基準

ICT 情報セキュリティ事務局は、当社における ICT 使用およびリモート接続に関わる基準を策定する。

4-2. ICT 情報セキュリティ活動計画

- (1) ICT 情報セキュリティ事務局は、当社における ICT 情報セキュリティマネジメントの活動計画を作成する。
- (2) 計画は、ICT 情報セキュリティマネジメントを遂行するために、従業員等への教育、ICT 使用およびリモート接続に関わる基準の遵守状況の点検、基準文書の見直しを含む。

4-3. ICT 情報セキュリティ教育

- (1) ICT 情報セキュリティ事務局は、ICT 情報セキュリティ推進担当者と連携して従業員等に対し ICT 使用およびリモート接続について継続的な社内教育を行う。
- (2) ICT 情報セキュリティ事務局は、ICT 情報セキュリティ推進責任者および ICT 情報セキュリティ推進担当者に対し、適宜必要な教育を行う。

4-4. ICT 情報セキュリティ自己点検

- (1) ICT 情報セキュリティ事務局は、ICT 情報セキュリティ推進担当者と連携して従業員等の ICT 使用およびリモート接続に関わる基準の遵守状況を定期的に点検する。

4-5. ICT 情報セキュリティ担当役員への報告

- (1) ICT 情報セキュリティ事務局は、従業員等の ICT 使用およびリモート接続に関わる基準の遵守状況、および ICT 情報セキュリティに関する例外事象の発生状況を ICT 情報セキュリティ担当役員へ報告する。

4-6. 基準文書の見直し

- (1) ICT 情報セキュリティ事務局は、教育や自己点検の結果を受けて、ICT 使用およびリモート接続に関わる基準の妥当性を評価すると共に、必要に応じて、内容の改訂を行う。

文書番号		セキュリティマニュアル	頁	6/8
------	--	-------------	---	-----

5. ITS の活動

5-1. 情報機器使用に関する基準

5-1-1. 申請の受理

ITS は、各部門から情報機器の設置、支給、貸出の申請があった場合、以下を確認し、問題がなければ受理する。

- (1) 申請書の必要事項がもれなく記載されていること。
- (2) 上記内容を申請者の所属長が承認していること。

5-2. システム使用許可に関する基準

5-2-1. ID の発行に関する基準

- (1) 申請者が社員であること。
- (2) 誓約書が提出されていること。
- (3) 共有 ID の場合、共有範囲が明確になっていること。
- (4) 所属長および ITS が承認していること。

5-2-2. 特権 ID の発行に関する基準

- (1) 申請者が社員であること。
- (2) システム管理が必要な部門であること。
- (3) ID 使用者から、誓約書の提出があること。
- (4) 承認者が所属長または ITS であること。
- (5) 社外の者に特権 ID を発行する場合、業務契約書や仕様書等で明記されていること。

5-2-3. 異動・退職時の ID の取扱

ITS は、各部門から、異動・退職の連絡があった場合、以下を確認して、異動・退職時の処理を実施する。

- (1) 所属部門からの連絡であり、所属長にも連絡されていること。
- (2) 異動・退職日が明確であること。
- (3) システムの異動・退職処理依頼日が明確であること。

5-2-4. アクセス制限に関する基準

- (1) 申請者が社員であること。
- (2) 承認者が所属長、または該当システムや共有エリアの管理者であること。
- (3) アクセス権付与の対象者が、社員、派遣であること。
- (4) 申請された権限(閲覧、作成・更新、削除 等)が、部門ごとのアクセス権の過去の設定状況と比較して、妥当と判断できること。

文書番号		セキュリティマニュアル	頁	7/8
------	--	-------------	---	-----

6. 例外事項

業務都合等により本基準の遵守事項を守れない状況が発生した場合は、ICT 情報セキュリティ担当役員に報告し、例外の適用承認を受けること。

7. 罰則事項

本マニュアルの遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。

文書番号		セキュリティマニュアル	頁	8/8
------	--	-------------	---	-----

改訂履歴表

版 数	制定・改訂日	実 施 日	改訂の概要 (改訂箇所、改訂内容、改訂理由等)	承 認	作 成
1	2019 年 4 月 1 日	2019 年 4 月 1 日	新規作成		