免責事項：このグローバルポリシーは機械翻訳を使用して翻訳されています。英語原文と本翻訳版の間に矛盾がある場合は、英語版が優先するものとする。

グローバルポリシー

IT グローバルポリシー

文書所有者	アグネタ・パルメール
バージョン	V3
取締役会にて採択	2023 年 12 月 18 日

1. 概要

ゲティンゲ・グループは、人と情報を保護すると同時に、IT リスク全体を軽減することをお約束します。このグループポリシーは、IT 分野におけるゲティンゲの立場を定義し、ユーザー、システム管理者、経営陣、IT セキュリティ担当者に期待する行動を明確にするものです。また、IT システムとアプリケーションの安全基準も設定しています。本方針は、ゲティンゲ・グループを代表して行動するすべての同僚および取引関係に適用されます。

2. 定義

本グローバルポリシーにおいて、以下の用語は以下の意味を有する：

産別会議	最高情報責任者
CISO	最高情報セキュリティ責任者
GDPR	一般データ保護規則（個人データ保護に関する EU 規則）
BYOD	Bring Your Own Device - ユーザー個人の PC、タブレット、携帯電話

3. スコープ

本グローバルポリシーは、すべてのゲティンゲ社、その子会社、および共同事業体（以下、総称して「ゲティンゲ」）に対して有効であり、ゲティンゲの施設内またはゲティンゲの指示の下で働く、当社のすべての従業員および取締役、ならびにコンサルタントおよび代理店要員（本グローバルポリシーでは、すべて「従業員」と呼びます）に適用されます。

本ポリシーの目的は、ゲティンゲ社内の IT に関する意思決定にガイダンスとサポートを提供することです。これは、受け入れられている最新の知識、ガイドライン、一般的な慣行に基づく、安全で許容される実践を反映した基準と手順を記述したものである。

4. 原則

コミットメントと期待

ゲティンゲの IT 体制は、IT 投資に対するリターンとリスクとリターンのバランスを取りながら、企業に IT サービスを提供することで価値を高めています。

ゲティンゲは、IT リスク全体を軽減しながら、人と情報の保護に取り組んでいます。私たちは、構造化された管理、一貫したプロセス、そしてビジネスとの強力な関係の構築を通じて、IT 機能を指揮・管理しています。

このポリシーの目的は以下の通りである：

- データと情報を保護する；
- ユーザー、システム管理者、管理者、IT セキュリティ担当者が期待される行動のルールを設定する；
- IT システムとアプリケーションの標準を設定する；
- IT リスク全体を軽減する。

当社は、ゲティンゲの IT システムまたはハードウェアにアクセスするすべての従業員および請負業者に、本ポリシーに従い、その高い基準を一貫して適用することを求めます。

5. IT リソースの許容可能な使用

許可された使用： ゲティンゲが提供する IT リソースは、適用される法律、規制、および業界標準に準拠した業務目的のためのものです。個人的な使用は、職務上の責任を妨げたり、他のポリシーに違反したりしない限り、容認されます。

禁止行為以下の行為を固く禁じます：

- IT システムやデータへの不正アクセス。
- 違法または無許可のソフトウェアの配布、所持、使用。
- 違法または非倫理的な活動に IT リソースを使用すること。
- データの不正な変更、破壊、開示。
- IT リソースを使用したハラスメント、差別、または組織の行動規範違反。
- ネットワークやデータのセキュリティを侵害する行為。

詳しいガイダンスについては、こちらをご覧ください：*IT アクセプタブル・ユース指令*

6. 情報セキュリティ

サイバーセキュリティ

私たちがサイバーセキュリティをどのように管理し、ゲティンゲのデジタル資産とデータを脅威から守るために必要なセキュリティ管理を確立するかを定義します：

- データや技術リソースを保護するためのルールやベストプラクティスを定義した、確立されたサイバーセキュリティ指令と手順を遵守する。
- 組織の情報システムとデータに影響を及ぼす可能性のあるサイバーセキュリティリスクを定期的に評価し、特定する。
- サードパーティベンダーやサービスプロバイダーに関連するサイバーセキュリティリスクを評価し、管理する。
- 不審な動きがないかシステムを定期的に監視し、セキュリティ監査を実施し、監査要件を遵守する。

サイバーセキュリティに関するすべての質問は、ゲティンゲの CISO に直接行うものとします。

さらなるガイダンスについては、こちらをご覧ください：*サイバーセキュリティ指令*

データ管理

- 従業員は、機密情報および機微情報を保護しなければならない。データは、ゲティンゲのデータ分類指令に従って分類され、取り扱われなければなりません。

詳しいガイダンスはこちらをご覧ください：*データ管理指令*

セキュリティ・インシデントの報告

- すべての従業員は、セキュリティインシデントまたはセキュリティ違反の疑いがある場合は、IT 部門または指定された IT 担当者に速やかに報告しなければなりません。

さらなるガイダンスについては、こちらをご覧ください：*サイバーセキュリティ・インシデント指令*

アイデンティティ・アクセス管理指令

- 機密性の高いシステムおよびデータへのアクセスが、強力な認証および承認メカニズムを使用して、許可された担当者のみに制限されるようにする。

詳しいガイダンスはこちらをご覧ください： *アイデンティティおよびアクセス管理指令*

リモートアクセスとモバイル機器

- ゲティンゲのネットワークへのリモートアクセスは、安全で許可された方法によってのみ許可されます。

トレーニングと意識向上

- 従業員は IT セキュリティ慣行に関する研修を受け、定期的に注意喚起を行い、意識を維持する。

7. IT 機器およびソフトウェア

IT オペレーション

安定的かつ効率的な IT サービスを提供するために、IT 運用のベースラインを確立する。

ネットワーク・セキュリティ管理、パッチおよび脆弱性管理、悪意のあるコード保護、ロギングおよびモニタリング、パーソナル・コンピューターおよびモバイル・デバイス管理などの分野をカバーしている：

- マルウェア対策：ゲティンゲのネットワークに接続されているすべての機器には、最新のアンチウイルスおよびアンチマルウェアソフトウェアがインストールされている必要があります。
- 電子メールのセキュリティ：統合されたシステムがゲティンゲのセキュリティ基準に準拠していることを保証する、IT 部門が承認した電子メールサービスのみを使用してください。
- 機器の使用ゲティンゲが提供する IT 機器は業務用です。ゲティンゲのネットワークに接続されているその他の機器は、セキュリティ基準に準拠している必要があります。
- ソフトウェアのインストール：ゲティンゲの機器にソフトウェアをインストールする場合は、IT 部門の許可を得る必要があります。ライセンスされたソフトウェアのみを使用する。
- システム、デバイス、アプリケーションを安全に構成して、攻撃対象領域を減らし、セキュリティリスクを最小限に抑える。

詳しいガイダンスについては、こちらをご覧ください：*IT 運用指令*

データのバックアップ

必要不可欠な業務を維持するための計画があることを確認する。

- すべての重要なデータは、データ損失を防ぐために定期的にバックアップする必要があります。従業員には、重要なデータが IT バックアップ・プロセスに含まれていることを確認する責任がある。

詳しいガイダンスについては、*こちらをご覧ください：IT バックアップとリカバリ指令*

IT ガバナンス

IT プロジェクトとサービスを効率的かつ安全に提供し、IT 機器とサービスのグローバルライセンスコンプライアンスを維持し、適正な購買慣行を維持する：

- すべての IT プロジェクトは、プロジェクト・ポートフォリオ管理プロセスを遵守し、適切な承認を受けなければならない。

- ソフトウェア・ライセンス契約のコンプライアンスを維持するためには、IT ライセンシング管理の慣行に従わなければならない。
- IT 調達管理手順は、すべての IT 関連調達活動に従うべきである。

詳しいガイダンスについては、こちらをご覧ください：*IT ガバナンス指令*

IT クラウド管理

クラウド・ソリューションやクラウド・サービスを選択、導入、運用する前に考慮すべき点を概説する：

- IT 部門はクラウドの購買プロセスに（できるだけ早い段階で）関与しなければならない。

詳しいガイダンスについては、こちらをご覧ください：*IT クラウド指令*

アプリケーション・セキュリティ

IT システムの開発または取得の初期段階で、セキュリティが統合されていることを確認する。

さらなるガイダンスについては、こちらをご覧ください：*アプリケーションセキュリティ指令*

8. 役割と責任

ゲティンゲの全従業員は、本方針を読み、理解し、遵守する責任があります。各従業員は、本ポリシーに従って行動する責任を負う、

各ラインマネージャーは、各チームメンバーが本方針および関連する指令、指示、ガ イドラインにアクセスできるようにする責任があります。

IT 分野における定期的な情報提供や研修、コンプライアンスのフォローアップを含む日々の強化は、IT 部門のサポートのもと、各マネージャーの責任の一部となっている。

グループポリシーに対する違反は、解雇を含む懲戒処分につながる可能性があります。

9. グローバル・ポリシーに対する違反 – 声をあげよう

懸念を表明することをためらってはならない。このグローバルポリシーの違反が疑われるゲティンゲの社員は、直属の上司、倫理・コンプライアンスオフィス、またはゲティンゲのスピークアップラインに問題を報告することが期待されています。Getinge Speak Up Line は、Getinge 社内および社外のウェブページでご利用いただけます。ゲティンゲでは、懸念を表明したり意見を述べたりする人に対するいかなる報復も認めません。

さらに見るグローバル・スピークアップと非報復指令

10. 指導と援助

IT ポリシーや IT 指令の一部（法律、規制、財務、技術など）に従わない理由がある場合は、例外申請書に記入してゲティンゲの最高情報セキュリティ責任者に送付する必要があり、リスクレベルによっては追加の承認が必要になる場合があります。

本グローバル・ポリシーに関するご質問は、CIO のペレ・ニルソンまでご連絡ください。

関連文書

- サイバーセキュリティ指令
- サイバーセキュリティ・インシデント指令
- IT アクセプタブル・ユース指令
- IT ガバナンス指令
- IT 運用指令
- IT バックアップ・リカバリ指令
- IT クラウド指令
- データ管理指令
- アイデンティティ・アクセス管理指令
- アプリケーション・セキュリティ指令
- IT セキュリティ例外申請