更新日：2022/07/08

#	大項目	小項目	ルール	対策	対象
1	情報資産の取り扱い	情報資産の公開範囲	情報資産は閲覧可能な範囲と管理方法を明確にし、関係者以外へ公開しないよう厳重に取り扱う。 ※尚、社外秘～極秘の情報を機密情報として取り扱う。 ・極秘（会社登記簿、会社印鑑証明 等） 保管方法：書類は常時金庫施錠。電子データは、コールドストレージに暗号化して保管。 閲覧範囲：役員に任命された責任者のみ可。 ・秘（個人情報 等） 保管方法：書類は常時施錠。電子データは、社内システムに暗号化を施して保管。 閲覧範囲：責任者及び責任者より任命された従業員のみ可。 ・社外秘（社内報、会議資料 等） 保管方法：書類は常時施錠。電子データは、当社が許可したクラウドストレージ（Googleドライブ 等）に保管。プライベート端末からのアクセスも可とする。 閲覧範囲：従業員のみ可。 ・一般 制限無し。	・閲覧範囲を明示する。 ・閲覧権限を明示する。	紙媒体、電子データ
2		顧客情報資産の取り扱い	顧客情報資産を取り扱う場合、以下の取り扱い場所に合わせた規定に従う。 ・自社内 当社の取り扱い規定（情報セキュリティ運用規定 [2章～13章] 等）に則る。 ・お客様先 お客様先の取り扱い規定に則る。また、規定の有無や内容に関わらず、顧客情報資産をお客様先以外の環境に持ち出すことは厳禁とする（SALTOアカウントのメールに送信すること 等） ただし、顧客の指示があった場合や顧客の許可を得た場合は例外とする（作業報告書や契約書 等）	・左記のルールを周知し、定期的に教育を行う。 ・定期的に確認を行う。	従業員
3		開示許可のない情報の取得禁止	自分に開示が許可された情報のみ取得し、開示された以外の情報取得の必要が生じた場合、必ず責任者に相談する。	・左記のルールを周知し、定期的に教育を行う。 ・取得した情報がある場合は、責任者や管理者に報告した上で適切に処理する。 ・社内システムの機密情報はアクセス権を設定し、インターネットからのアクセスを制限する。	従業員、紙媒体、電子データ
4		機密情報の保管	機密情報の取扱者は、機密情報の保管場所（キャビネットなど）と保管方法、保管期限を定め、厳重に保管する。保管庫の施錠管理を徹底する。	・ロッカー、キャビネットなど所定の保管庫に格納する。 ・保管庫の施錠管理を徹底する。 ・保管場所に機密情報を保管していることを推測できるような表示をしない。 ・保管庫が足りているか確認する。	情報資産（物理・電子データ）
5		機密情報の持ち出し	機密情報を社外に持ち出すことは原則禁止とする。 ただし、業務上やむを得ず社外に持ち出す場合は、以下のルールを厳守する。 ・お客様先などに持ち出しが必要な場合、責任者の許可を得た上で持ち出しを行う。 ・使用目的を明確にし、必要最小限に留め、目的以外の使用を禁止する。 ・移動中は常に肌身離さず携行する。 ・書類は、外から閲覧できないように封筒などに入れ、他の書類と混ざらないようにする。 ・電子データは、可能な限り秘匿化を行い、ハードディスクロック、ファイルロック、暗号化などを利用する。	・持ち出し不可の情報は情報資産の公開範囲に準拠する。 ・必要以上に情報を持ち出していないか確認する。 ・持ち出す可能性が高い機密情報の一覧 営業部：経歴書、スキルシート、顧客情報、企業情報、お客様から頂いた名刺、契約書 等 管理部：給与明細、契約書、法務・税務・労務関連 等 技術部：顧客情報、プロジェクト資料（設計書、データ 等）	情報資産（物理・電子データ）
6		機密情報の漏洩・改ざん禁止	機密情報の漏洩、改ざんにつながる行為を禁止する。 漏洩、改ざん行為を見つけた場合は、管理者に報告する。	・左記のルールを周知し、定期的に教育を行う。 ・漏洩、改ざん行為を見つけた場合は、管理者に報告する。	従業員、電子データ
7		個人情報の取り扱い	個人情報保護ルールに従い、個人情報秘匿化を行った上で取り扱う。	・個人を特定できないよう加工（名前のイニシャル化）する。 ・社外に持ち出す際は必ず秘匿化など、漏洩対策を講じる。	情報資産（物理・電子データ）
8		本人への情報の開示	機密情報を提示する際は、確実に相手だけにわかる方法を用いる。	・機密情報は直接手渡しや本人宛に郵送するなど確実な方法を使用する。 ・機密情報に該当する問い合わせがあった際は、当社の従業員であっても本人確認としてチャットやメールで連絡を行う。	情報資産（物理・電子データ）
9		本人不在時の情報の提供	本人不在時は、不用意に本人の機密情報を第三者に開示してはならない。 但し、以下の場合は例外とする。 ・本人の代理で行う場合 本人の許可を取り適切な方法と公開範囲内で提供する ・機密情報に該当しない場合 本人許可は不要とする。（名刺に記載されている社用携帯番号等）	・本人不在時の機密情報に該当するお問い合わせがあった場合、本人に機密情報の提供について必ず確認を行う。 ・事前に本人から提示許可を受けている場合は、決められた範囲内である事と且つ問い合わせ相手が特定できる場合に限る。	情報資産（物理・電子データ）
10	日常業務のルール	日常会話	・社外でのお客様情報や個人情報の発言は、特定されないように注意する。 ・エレベータ内では、第三者と同乗の場合はマナーを考慮し私語を禁止とする。	・社外で発言する際は周り人がいなくても、業務に関連する社名や人名は、イニシャルや俗称など曖昧な表現で行う。 ・発言者が気づいていない場合、周囲の人が注意を行う。	従業員

更新日：2022/07/08

#	大項目	小項目	ルール	対策	対象
11		席から離れる際	離席時は書類または業務端末の機密情報が閲覧されないよう対策する。	・据置型の業務端末（PC 等）から離れる際は必ず操作できないように画面をロックする。無操作状態が5分続くと自動ロックをするように設定する。 ・携帯型の業務端末（スマートフォン 等）は必ず持ち歩く。 ・書類は重要度に限らず、机の上に放置しない。離席する場合は、書類が目に見えないようしまう。（キャビネットやバインダーなど）	情報機器、書類
12		セキュリティカードの取り扱い	セキュリティカードは各自紛失しないように対策する。 ※社外でセキュリティカードを貸与された場合は、現場のルールに従う。	・勤務中は必ずストラップに入れて着用する。 ・チャック付きの鞄に入れ、鞄を手から離さないようにする。 ・保管場所（移動中や在宅時）を決め、管理を徹底する。	セキュリティカード
13		セキュリティカードの貸し借り	本人所有のセキュリティカードを他人に貸すことを禁止する。	・左記のルールを周知し、定期的に教育を行う。	セキュリティカード
14		自己判断・自己解釈の禁止	規定やセキュリティルール上で明文化されていないことに関して、暗黙的に許可されていると解釈や判断せず、迷った場合は責任者に必ず確認する。	・左記のルールを周知し、定期的に教育を行う。	従業員
15	オフィス環境	帰宅時の確認	帰宅時は、情報機器や書類を保管場所（キャビネット等）に格納する。 机の上に情報機器や書類などが置かれていないことを確認してから帰宅する。 特に最終退出者は、施錠が確実にされていることを再度確認する。	・PCをロッカーや所定の場所に収納する。 ・書類をキャビネットに収納する。 ・最終退出者は施錠を行った後、施錠が確実にされていることを確認する。	情報機器、紙媒体
16		エリア区切り	セキュリティゲートによってセキュリティエリアを区切り、入室記録を管理する。 ※会議室は、セキュリティエリア外のため、対策は不要。	・会議室は、セキュリティエリア外のため、対策は不要とする。 ・事務所は、原則従業員のみが利用でき、セキュリティゲートで入室者を管理する。	会議室、事務所
17		セキュリティエリア内 （事務所内／事務所入退室）	・事務所への入退室時は、セキュリティカードを必ず各自が使用して入退室する。 ・事務所内でセキュリティカードを着用していない人を見かけた場合、確認を行う。	・事務所内でセキュリティカードを着用していない人を見かけた場合、確認を行う。 ・入退室時は各自セキュリティカードを認証装置に通し、共連れを禁止する。 ・セキュリティカードを未所持の人をやむを得ず入室させる際は、申請を行い管理部の承認を受ける。	従業員、セキュリティカード
18		社内システムの利用	社内システム（VPN接続も含む）に接続する場合、以下のルールに従う。 ・会社から貸与された業務端末を利用 ・リモートワークなどでインターネットを経由して接続する場合、必ずVPNを利用	・社内システムの範囲を定義する。 ルータ：FortiGate 業務用サーバ：ADサーバ、ファイルサーバ LESALTO用サーバ：開発サーバ、Webサーバ、APIサーバ 等 ・定期的に確認を行う。	情報機器
19	リモートワーク環境	使用端末	リモートワークに使用する業務端末は、管理者の承認を得たものに限定し、それ以外の使用を原則として禁止とする。 ただし、一時的に社内業務で利用する場合、利用範囲と用途を限定した上で利用可とする。 ・利用範囲 Google Workspace、Slack、Zoom 等 ・用途 オンライン会議、帰社日 等	・業務端末を一覧化して管理する。 ・定期的に確認を行う。	情報機器
20		社内システムへの接続	社内システム環境への接続は、管理者が指定した方法で行い、許可なく設定等を変更しない。	・定期的に確認を行う。	情報機器
21		作業環境上の注意（自宅）	自宅でリモートワークを行う場合、社外利用と同等の対策を行うこととする。 ・プライベートネットワークの設定を禁止する。 (接続したネットワーク上にPCが検知されないようにする) ・公共のWi-Fiの利用は禁止する。 ・覗き見防止対策を行う。 ・音声が外に漏れないようにする。 ・業務空間とプライベート空間を可能な範囲で仕切る。 ・空き巣など被害にあわないよう、可能な範囲で防犯対策を行う	・持ち出す可能性のある業務端末に覗き見防止フィルムを導入する。 ・定期的に確認を行う。	従業員
22		作業環境上の注意（自宅以外）	自宅以外でリモートワークを行う場合、社外利用と同等の対策を行うこととする。 ・プライベートネットワークの設定を禁止。 (接続したネットワーク上に PCが検知されないようにする) ・公共のWi-Fiの利用は禁止。 ・共同スペースでの業務は原則禁止。 個室などの第三者が介在しない区切られた空間で行う。 ・覗き見防止対策を行う。 ・音声が外に漏れないようにする。 ・業務端末を置いて席を離れる場合、施錠ができる場所に保管。 施錠ができない場合は、業務端末を持ち歩く。	・持ち出す可能性のある業務端末に覗き見防止フィルムを導入する。 ・定期的に確認を行う。	従業員
23		文書の管理	機密情報の印刷は、原則として禁止する。 業務上やむを得ず、印刷する場合は責任者の許可を得る。	・左記のルールを周知し、定期的に教育を行う。	紙媒体
24		電子データ（情報資産）の管理	社内の情報資産または顧客情報資産を取り扱う場合、第三者に情報が漏れないように以下を禁止する。 ・不要な電子データの取得 ・社内用の業務端末やお客様から貸与された業務端末で、許可されていない業務外の利用	・左記のルールを周知し、定期的に教育を行う。	従業員
25	文書（物理）	紛失、盗難の防止	文書を保管場所以外に置く場合（印刷、コピー、閲覧など）は、目的以外の行動をしないようにする。 また、書類を紛失しないように取り扱う。他の書類と混ざらないよう注意する。	・展示を行い、日常的に意識付けする。 ・他の書類と混ざらないように管理する。 ・周囲で左記のルール違反を見かけた場合は注意する。	紙媒体

更新日：2022/07/08

#	大項目	小項目	ルール	対策	対象
26		文書の破棄	不要な文書は、できるだけ速やかに復元不可能な手段で廃棄する。また、裏紙の使用を原則禁止とする。	・不要になった書類はシュレッダーにかける。	紙媒体
27		荷物の配送	誤配送を行わないよう、送り先を確認してから配送する。	・封入物のダブルチェックを行う。 ・住所のダブルチェックを行う。	配送物
28		FAXの送信	誤送信を行わないよう、FAXの宛先を確認してから送信する。	・送信先を厳重に確認するようルールを周知する。 ・複合機の前に注意喚起の張り紙を張る。	FAX
29	文書（電子データ）	電子データの破棄	用途が無くなった、または長期間使用しない情報資産は速やかに削除する。 不要になった電子データはゴミ箱に捨てたままにせず、完全に削除する。	・左記のルールを周知し、定期的に教育を行う。	電子データ
30		電子データのアクセス権	権限が与えられていない電子データへの不正アクセスを禁止する。 管理者は情報資産の公開範囲に基づいて、適切なアクセス権を設定する。	・社内システムの機密情報はアクセス権を設定し、インターネットからのアクセスを制限する。 ・アクセス権を付与できる管理者を絞り、アクセス権を変更する場合は適切であることを責任者に確認する。	電子データ
31		WEBサービスと機密情報の取り扱い	機密情報をWEBサービスに公開設定でアップロードすることを禁止する。 （例） ・掲示板サイト（5ちゃんねる、したらば等） ・SNS（Twitter、Facebook等） ・QAサイト（Teratail等） ・クラウドストレージ（OneDrive、iCloud等） ・ソースコード共有サービス（GitHub等） ・ブログサイト（Amebaブログ、Qiita等） ・動画投稿サイト（YouTube、ニコニコ動画等）	・WEBサービスの利用にあたり、コンプライアンスとセキュリティ啓蒙のための活動を行う。 ・アップロードする場合は、公開設定に注意する。	従業員、電子データ
32		WEB発信	業務上知り得た些細な情報であってもWEBで発信することを禁止する。 業務上やむを得ずWEBで発信する場合は、届け出を行う。 機密情報の有無に限らず、発信内容については細心の注意を払う。 無許可で会社の公式を名乗り、WEBサービスを利用することを禁止する。	・私的なWEBの利用にあたり、コンプライアンスとセキュリティ啓蒙のための活動を行う。 ・業務上でやむを得ずWEBで発信する場合は、必ずダブルチェックを行う。 ・左記のルールを周知し、定期的に教育を行う。	従業員、電子データ
33	業務用情報機器（PC、サーバー）	ウィルス対策	業務端末にウイルス対策ソフトウェアを導入し、定期アップデートと常時検知を行う。 常時検知を行い、定義ファイル・ソフトウェアを最新の状態に保つ。定期的に全量検査を行う。	・ウィルス対策ソフトウェアを導入し、定期アップデートと常時検知を行う。 ・定期的に全量検査を行う。	情報機器
34		禁止対象のソフトウェア	業務端末に以下のソフトウェア（アプリも含む）のインストールを禁止する。判断に迷った場合、必ず責任者に確認する。 （例） ・P2Pファイル共有（Winny、BitTorrent 等） ・偽装された、または悪意のあるソフトウェア（PCKeeper、solvusoft 等） ・業務上不要なソフトウェア ・脆弱性が報告されているソフトウェア ・社で管理しているものと競合するソフトウェア（ウィルス対策、暗号化、VPN 等）	・禁止対象のソフトウェアのリストを作成し掲示する。 ・判断がつかないソフトウェアをインストールする場合は、必ず責任者の承認を受ける。 ・禁止対象のソフトウェアが業務端末にインストールされてないか監査する。 ・左記のルールを周知し、定期的に教育を行う。	情報機器、ソフトウェア
35		ソフトウェアのインストール	業務端末にソフトウェアをインストールする場合、以下のルールに従う。 ・ソフトウェアを導入する場合、禁止対象でないことを確認した上で責任者の許可を得る。 ・ソフトウェアをダウンロードする場合、正式な場所（公式サイト、公式アプリケーションストア）であることを確認した上で責任者の許可を得る。	・左記のルールを周知し、定期的に教育を行う。	情報機器、ソフトウェア
36		ソフトウェアのアップデート	業務端末にインストールされたソフトウェアを常に最新化（アップデート、パッチをあてる等）を行う。	・定期的にソフトウェアのバージョンや更新情報、サポート期間などを確認する。	情報機器、ソフトウェア
37		私的利用の禁止	業務端末の私的利用を禁止する。 私的利用は業務と無関係な利用インターネットの閲覧、電子メールの使用、チャットなどを含む。	・左記のルールを周知し、定期的に教育を行う。	情報機器
38		私用アカウントの業務利用	私用アカウントを業務用情報機器で使用することは原則禁止する。 会社から貸与されたアカウント（例：google ／ 〇〇@salto.link）以外を業務に使用する行為を指す。	・左記のルールを周知し、定期的に教育を行う。	情報機器
39		紛失と盗難の防止	社外での使用時は紛失や盗難を避けるため、常に手の届く状態で持ち歩く。社外でパソコンを置いたまま離れることを禁止する。	・持ち出す可能性のある業務端末に覗き見防止フィルムを導入する。 ・左記のルールを周知し、定期的に教育を行う。	情報機器（パソコン）
40		個人所有の情報機器の取り扱い	・業務エリア内への個人所有の情報機器の持ち込みは許可とするが、社内LANへの接続および社内の情報機器への接続は禁止する。 ・個人所有の情報機器で秘以上の情報へのアクセス及び情報の保有を禁止する。	・社内のネットワーク環境を利用する場合は、必ず管理部（情シス）に確認をする。 ・左記のルールを周知し、定期的に教育を行う。	情報機器（パソコン）
41		記憶媒体の取り扱い	・記憶媒体を破棄する場合、専門の業者へ依頼し、物理的に破壊する。 ・私物の外部記憶媒体の持ち込みを禁止する。 ・外部記憶媒体の利用が業務上必要な場合、管理者の承認を得て貸与する。	・不要となった記憶媒体は専門の業者へ依頼し、物理的に破壊する。 ・左記のルールを周知し、定期的に教育を行う。	記憶媒体（HDD、SSD、空のCD・DVD-R/RW、USBメモリ、NASなど）
42		ID/パスワードの共有	会社から個人に貸与されたID/パスワードを他人に教えることを禁止する。 ログイン状態で貸し出すことを禁止する。	・左記のルールを周知し、定期的に教育を行う。	従業員、ID/パスワード
43		ID/パスワードの管理方法	ID/パスワードは、情報端末への保存を禁止する。パスワードの取り扱いを注意する。	・パスワードが書かれたメモや付箋紙、及びデータがパソコンの周囲及びデスクトップ等、第三者が容易に視認できる場所にないか確認し、従業員同士で注意喚起を行うよう指導する。	従業員、ID/パスワード

更新日：2022/07/08

#	大項目	小項目	ルール	対策	対象
44		ID/パスワードポリシー	強固で推測されないパスワードを使用し、定期的に変更を行う。	①パスワードの設定 英小文字、英大文字、数字、記号（_-!%$#=+のみ使用可）の内2種類を1文字入れて6文字以上で設定する。 ②以下のパスワードの禁止事項を周知する。 ・辞書に登録されている単語等（password、admin 等） ・単純な文字な羅列（1234abc 等） ③変更の頻度 定期的にパスワードの変更を実施する。	従業員、ID/パスワード
45	業務用情報機器（携帯）	私的利用	会社から貸与された業務用携帯の私的利用を禁止する。但し、私用携帯が使用できず、かつ緊急の場合（社会的通念上の人道的な行い）は可能とする。	・左記のルールを周知し、定期的に教育を行う。	従業員、携帯
46		紛失、盗難の防止	紛失や盗難を避けるため、常に携帯する。紛失した場合は至急停止措置を実施する。	・左記のルールを周知し、定期的に教育を行う。	携帯
47	電子メール	電子メールの誤送信対策	電子メールの送信前に、宛先が正しいことを確認する。 機密情報を含むファイルを外部に送信する場合、添付ファイルにパスワードをかけてから送り、パスワードは別送する。	・左記のルールを周知し、定期的に教育を行う。 ・Gmailで「送信取り消し設定」を各自で設定する、手順を配布する。	電子メール
48		発信元が不明なメールの開封	発信元が不明なメールは開封しない。	・左記のルールを周知し、定期的に教育を行う。	電子メール
49		不審メールの報告	送信元が明確でも、不審に感じたメールの（添付ファイルやURLリンク 等）は開かず、責任者へ速やかに報告する。	・左記のルールを周知し、定期的に教育を行う。	電子メール
50	緊急時の対応	事故対応カードの携帯	「事故発生・緊急時における連絡先一覧カード」を常時携帯する。	・左記のルールを周知し、定期的に教育を行う。	従業員（セキュリティ事故対応カードの所持）
51		セキュリティ事故発生時の対応	セキュリティ事故発生時は事故対応カードに記載されているフローに従い、連絡先に電話連絡を行い指示を仰ぐ。 24時間365日いかなる場合であっても連絡が繋がるまで繰り返す。	・左記のルールを周知し、定期的に教育を行う。	従業員（セキュリティ事故対応のフロー）