情報セキュリティ基本規程

（目的）

第１条 本規程は、一般社団法人ディレクトフォース（以下、“DF”）の「情報セキュリティポリシー／基本方針」に基づき、当社団における情報セキュリティの維持および推進を行うために必要な基本的事項を定めたものであり、当社団における情報セキュリティマネジメントシステム（組織的に情報セキュリティの維持および向上のための施策を立案、運用、見直しおよび改善すること）を確立することを目的とする。

（定義）

第２条 本規程における用語の定義は、次の各号に定めるとおりとする。

(1) 「情報」とは、有形、無形を問わず、当社団が保有する一切の情報（当社団固有の情報の他、契約その他の正当な手段に基づき入手した、会員およびその他の第三者から取得した情報を含む。）をいう。

(2) 「情報資産」とは、有形、無形を問わず、情報を含む媒体と伝達手段をいう。全ての紙面、記憶媒体、情報システム等と、口頭や電気通信等で伝達される情報を含む。

(3) 「情報システム」とは、情報を取扱う機器装置等のハードウェア、ソフトウェア、プログラム、伝送経路等および、これらにより構成される電子システムおよびその収納施設等をいい、情報に関連する一切の資産および処理方法を含む。

(4) 「リスク」とは、想定される脅威（情報資産に対して損害を与える要因をいう。以下同じ。）が、情報資産に対して損害を与える可能性をいう。

(5) 「情報セキュリティ」とは、情報資産に対し、
①機密性（正当に許可した者だけ が当該情報資産にアクセスできること）、②完全性（正確および完全であるよう、 情報資産を不正な改ざんおよび破壊から保護すること）および③可用性（正当にアクセスを許可された者が、使用許諾の範囲内で、必要なときに円滑に当該情報資産 にアクセスできること）を確保し維持することをいう。

(6)「サイバーセキュリティ事案」とは、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やサイバー攻撃等の、サイバーセキュリティが脅かされる事案をいう。

(7) 「対象情報」とは、情報セキュリティの確保および維持が必要と判断した情報をいう。

(8) 「対象情報システム」とは、情報セキュリティの確保および 維持が必要と判断した情報システムをいう。

(9)「対象情報資産」とは、対象情報および対象情報システムの総称をいう。

(10)「不測事態」とは、情報セキュリティの確保および維持に重大な影響を与える災害、障害、セキュリティ侵害等の事態をいう。

(11)「従事者等」とは、「DF 個人情報保護基本規程」に定めた当社団の業務に従事する全て

の者をいう。

（適用範囲）

第３条 本規程は、DF のすべての従事者等に適用する。

（情報セキュリティ管理体制）

第４条 当社団は、情報の機密性、完全性、可用性を維持するために、「情報セキュリティ委員会」を設置、その役割・責任を下記の通り明確にする。

２．理事会は、システムリスクの重要性を十分に認識した上で、システムを統括管理する理事を定める。なお、当該役員はシステムに関する十分な知識・経験を有し業務を適切に遂行できる者であることが望ましい。

３．「情報セキュリティ委員会」は、個人情報保護管理者により構成されるものとする。

４．情報セキュリティ委員会は、当社団における情報セキュリティ維持および向上に必要な基準、規程類を制定し、これらの周知徹底、運用および見直し、改善を図るとともに、施策等の審議、評価、見直し、および改善を行う。

５．情報セキュリティ委員会は、情報セキュリティに関する不測事態が生じた場合の連絡体制を整備、運営および見直し、改善を行う。

６．情報セキュリティ管掌理事とは、理事会の決議に基づき理事の中から選任された者であって、当社団における情報セキュリティに係る業務について情報セキュリティ実施手順書に記載した統括的責任と権限を有するものとする。

７．情報セキュリティ管掌理事は、情報セキュリティ委員会の委員長を務めるものとする。

８．情報セキュリティ委員会メンバーは、当社団の情報セキュリティを本規程に従い、当社団における情報セキュリティに係る業務を実施する。

（対象情報資産に関する情報セキュリティ）

第５条 従事者等は、自己が扱う対象情報資産を適切に管理しなければならない。

２．従事者等は、対象情報資産の管理にあたり、「DF 個人情報保護基本規程」その他の情報セキュリティに関連する規程類を遵守しなければならない。

３．情報セキュリティ委員会は、関係部署と協議のうえ、従事者等が対象情報資産を適切に管理するために必要な事項等を定めた基準および規程等を制定し、周知徹底、運用を行い、定期的またはシステム基盤等の変更の都度、見直し、改善を図る。

４．情報セキュリティ委員会は、前項に基づき制定された基準および規程類に従い、従事者等が、対象情報資産を適切に管理するよう、周知徹底、運用を行い、指示を

行う。

５．従事者等は、対象情報資産の使用および管理に際し、情報セキュリティに関連する規程、要領等を遵守しなければならない。

（対象情報システムに関する情報セキュリティ）

第６条 情報セキュリティ委員会は、当社団の保有する対象情報システムについて、その導入、運用、保守を通じ、対象情報システムの重要度や特性に適合した情報セキュリティの確保、維持のための施策（コンピュータウィルスからの保護、記録情報のバックアップ、情報システムの運用の記録、ネットワークの管理、情報システムの付属媒体の管理、電子メールのセキュリティ、アクセス制御、不正アクセス対策を含むが、これらに限らない。）を講じるものとする。

２．情報セキュリティ委員会は、対象情報システム、ネットワーク等のサイバーセキュリティに対し、サイバー攻撃の施策（ファイヤウォールの設置、抗ウィルスソフトの導入、 脆弱性診断、これらに限らない。）を講じるものとする。

３．情報セキュリティ委員会は、システム、データ、ネットワーク管理上のセキュリティに関して統括を行う。

４．情報セキュリティ委員会は、コンピュータシステムの不正使用防止対策、不正アクセス防止対策、コンピュータウィルス等の不正プログラムの侵入防止対策等を行う。

5. 従事者等は、対象情報システムの利用および管理に際し、情報セキュリティに関連する規程、要領等を遵守しなければならない。

第７条 情報セキュリティ委員会は、対象情報資産を取引先等の第三者に開示する場合、対象情報資産を第三者に預ける場合、その他第三者が対象情報資産を知り得る場合は、当該第三者との間で情報セキュリティの確保、維持のために必要な契約を締結する等の適切な措置を講じなければならない。

２．情報セキュリティ委員会は、前項の場合、当該第三者による当該対象情報資産の適切な情報セキュリティの確保、維持のために必要な監督に努める。

３．情報セキュリティ委員会は、関係部会・研究会・同好会の世話役と協議のうえ、取引先等の第三者との契約に関する基準および規程類において、第１項に定める適切な措置を講じるために必要な事項等を確保するとともに、これにかかる周知徹底、運用および見直し、改善を図る。

（保管環境に関する情報セキュリティ）

第８条 情報セキュリティ委員会は、対象情報資産を保管する建物、区画、書棚等について、当該対象情報資産につき不当なアクセス、紛失、盗難等を防止するため、管理区域の入退出管理その他の適切な措置を講じるものとする。

２．情報セキュリティ委員会は、関係部会・研究会・同好会の世話役と協議のうえ、前項に基づき基準および規程類を定め、これにかかる周知徹底、運用および見直し、改善を図る。

（不測事態対応計画）

第９条 情報セキュリティ委員会は、不測事態が生じた場合においても、事業活動に支障を来さない、又は支障を最小限化するための計画（以下「不測事態対応計画」という。）を立案、策定、周知および見直し・改善を行うものとする。

２．情報セキュリティ委員会は、不測事態対応計画の実効性について定期的に見直し、必要に応じ改善を図るものとする。

３．情報セキュリティ委員会は、関係部会・研究会・同好会の世話役と協議のうえ、不測事態対応計画の策定等を行うために必要な事項等を定めた組織基準を制定し、情報セキュリティ委員会に付議、この周知徹底、運用および見直し、改善を図る。

４．代表理事及び管掌理事は、システム障害等発生の危機時において、果たすべき責任やとるべき対応について具体的に定める。

（不測事態の報告等）

第１０条　　従事者等は、不測事態の発生又は発生の兆候を知った場合、直ちにこれを所属する情報セキュリティ委員会に報告するものとする。

２．情報セキュリティ委員会は、前項の報告を受けた場合、速やかに不測事態対応計画を実行するとともに、当該不測事態の原因究明を行う。また、不測事態の発生等につき、管掌理事に報告ものとする。

３．情報セキュリティ委員会は、情報セキュリティ管掌理事の指示に基づき、関係部門・研究会・同好会の世話役と協議のうえ、当該不測事態の対応を行い、事態の収束を図るものとする。

４．情報セキュリティ委員会は、不測事態の再発防止の観点から、不測事態への対応結果につき、必要に応じ情報セキュリティ管掌理事に報告する。

附 則　１．この規程は、2023 年４月１日より施行する。