

上海艾杰飞人力资源有限公司

個人情報取扱規程

開示版

情報安全管理室

2021年11月1日から実施

上海艾傑飛人力資源有限公司

個人情報取扱規程

第1章 総則	3
1.1 目的	3
1.2 用語および定義	3
1.2.1 個人情報	3
1.2.2 本人	4
1.2.3 本人の同意	4
1.2.4 求職者	4
1.2.5 個人情報の取扱	4
1.2.6 個人情報保護マネジメントシステム	4
1.2.7 不適合	4
1.3 個人情報保護マネジメントシステムの運用	4
1.3.1 運用手順の明確化	4
1.3.2 適用法令等	5
1.3.3 個人情報保護方針	5
1.3.4 内部の管理制度及び操作規程	5
1.3.5 責任および権限	5
1.3.5.1 個人情報安全責任者（総経理）	5
1.3.5.2 個人情報取扱責任者	6
1.3.5.3 情報システムセキュリティ担当	6
1.3.6 個人情報の特定	6
1.3.6.1 個人情報の管理	6
1.3.7 リスク等の認識、分析および対策	6
1.3.8 個人情報の取扱いに関する事故への対応	7
1.3.8.1 事故の把握と対応の決定	7
1.3.8.2 通知・公表	7
1.3.8.3 事故の対応実施	7
1.3.8.4 事後処理	8
第2章 個人情報の取得、利用および提供に関する措置	8
2.1 利用目的の特定	8
2.2 適正な取得	8
2.3 機微な個人情報の取得、利用および提供の制限	8
2.4 個人情報の取扱に関する措置	9
2.5 個人情報の公開に関する措置	10
2.6 個人情報の提供等に関する措置	10
2.7 個人情報の域外提供に関する措置	10
第3章 個人情報の適正管理	10

3. 1	正確性の確保	10
3. 2	安全性の確保	10
3. 3	従業員等の責務	11
3. 4	個人情報の保存および廃棄	11
3. 4. 1	保存および安全管理	11
3. 5	情報システムセキュリティ	11
3. 5. 1	コンピュータ機器等の管理	11
3. 5. 2	情報システムの論理的保護	12
3. 5. 2. 1	認証	11
3. 5. 2. 2	暗号の利用	11
3. 5. 2. 3	セキュリティ監視と維持	11
3. 5. 2. 4	バックアップ	12
3. 5. 2. 5	ウイルスチェック	12
3. 5. 3	ネットワークの管理	12
3. 5. 4	情報システムの廃棄	13
3. 6	個人情報の委託処理に関する措置	13
3. 7	合規性監査	13
第4章	個人情報に関する本人の権利	13
4. 1	個人情報取扱行為における個人の権利	13
4. 1. 1	知る権利と決定権	13
4. 1. 2	閲覧、複製、移転	13
4. 1. 3	訂正と補充	14
4. 1. 4	削除	14
4. 2	個人による権利行使	14
第5章	個人情報の取扱いに関する教育・研修	14
5. 1	教育・研修の実施	14
第6章	個人情報保護影響評価の実施・記録作成・保存	15
6. 1	個人情報保護影響評価の実施・記録作成	15
6. 2	個人情報影響評価の内容	15
6. 3	個人情報保護影響評価報告及び取扱状況の保存	15
第7章	苦情、相談および問い合わせへの対応	15
7. 1	苦情、相談および問い合わせに関する受付窓口の設置	15
7. 2	苦情、相談および問い合わせの内容の記録と報告	16
7. 3	重大案件への対応	16
第8章	その他	16
8. 1	罰則	16
8. 2	規程の改廃	16
8. 3	疑義取扱	16
第9章	付則	17

第1章 総則

1. 1 目的

この規程は、上海艾杰飞人力资源有限公司（以下「RGF」という。）が保有するすべての個人情報適切に取扱うために必要な事項を定める。RGFは、取扱う個人情報の価値とリスクを認識し、RGFが保有するすべての個人情報が適切に取扱われている状態を確立し、これを維持、発展させることを目指す。本規程は、RGFのすべての役員および従業員に適用する。RGFのすべての役員および従業員は、本規程を遵守し、個人情報を適切に取扱うとともに、RGFが保有するすべての個人情報の漏洩防止のために細心の注意を払わなければならない。なお、RGFが保有する個人情報を取扱う業務に携わる臨時社員（アルバイト、実習生も含む）、派遣社員および業務委託員（RGFと業務委託契約を締結した法人の従業員も含む。）についても、本規程を準用する。（本規程において、RGFの役員および従業員、RGFの業務に携わる臨時社員、派遣社員ならびに業務委託員を総称して「従業員等」という）。

1. 2 用語および定義

1. 2. 1 個人情報

次の個人情報をはじめ、RGFが取得するすべての個人情報をこの規程の対象とする。個人情報には、電子的方式又はその他の方式により記録され、すでに識別され又は識別可能な、自然人と関連する各種の情報が含まれる。ただし、匿名化（個人情報に処理を施すことにより、特定の自然人を識別することができず、かつ復元することができなくなるプロセスをいう）処理された情報は含まれない。

(1) 求職者の個人情報

この規程を適用する求職者の個人情報（以下「求職者情報」という。）の範囲は、RGFがその業務の過程で取扱うすべての求職者情報とする。

(2) 取引先従業員の個人情報

この規程を適用する取引先従業員の個人情報（以下「取引先従業員情報」という。）の範囲は、求人企業や取引先の従業員情報に限定し、RGFが取引をする、または取引を検討している企業や団体の従業員の個人情報をいう。

(3) 従業員等の個人情報

この規程を適用するRGFの従業員等の個人情報（以下「従業員情報」という。）の範囲は、すべての役員および従業員の個人情報、臨時社員および業務委託員の個人情報ならびにRGFが雇用管理を行う上で取扱う派遣社員の個人情報とする。なお、派遣社員については、本来、「労働契約法」等に基づき派遣元により派遣社員の個人情報が一括管理されるため、RGFとしては、適切な方法で派遣社員の個人情報を取扱う。

1. 2. 2 本人

本人とは、個人情報により識別され、又は関連付けられる自然人をいう。

1. 2. 3 本人の同意

本人の同意とは、本人が、個人情報の取扱いに関する情報を与えられた上で、自己に関する個人情報の取扱いについて同意する意向を表明することをいう。当事者が民事行為能力を欠く者の場合は、法定代理人等の同意も得なければならない。

1. 2. 4 求職者

求職者とは、RGF から転職についての助言や具体的なサポートを受ける個人をいう。

1. 2. 5 個人情報の取扱

個人情報の取扱には、個人情報の収集、保存、使用、加工、伝送、提供、公開、削除等が含まれる。

1. 2. 6 個人情報保護マネジメントシステム

個人情報保護マネジメントシステムとは、RGF が自らの業務において使用する個人情報について、その有用性に配慮しつつ、個人の権利や利益を保護するための方針、体制、計画、実施、点検および審査を含むマネジメントシステムをいう。

1. 2. 7 不適合

不適合とは、中華人民共和国の「民法典」、「個人情報保護法」および「ネットワーク安全法」など個人情報保護に関連する法令の要求を満たしていないことをいう。

1. 3 個人情報保護マネジメントシステムの運用

1. 3. 1 運用手順の明確化

RGF は、その情報保護マネジメントシステムを確実に実施するために運用の手順を明確にする。

1. 3. 2 適用法令等

- (1) RGF は、個人情報を取扱うにあたり、「民法典」、「個人情報保護法」、および「ネットワーク安全法」等の関連する法律、法規、規則、政策を遵守する。
- (2) 情報安全管理室は、RGF の個人情報保護に関連する法令等の最新版を個人情報取扱責任者の承認を得たうえで、役員・従業員及び外部スタッフが必要に応じて参照出来るように保存する。

1. 3. 3 個人情報保護方針

- (1) 個人情報安全責任者（総経理）は、明確な個人情報保護の理念に基づき、次の事項に関連する個人情報保護方針を定めるとともに、これを実行し維持する。
 - a) 事業の内容および規模を考慮した適切な個人情報の取扱いに関する事
 - b) 個人情報への不正アクセス、個人情報の漏洩、滅失または毀損の防止に関する事
 - c) 苦情、相談および問い合わせへの対応に関する事
 - d) 個人情報の取扱いに関する法令、国が定める指針およびその他の規範を遵守すること。個人情報保護マネジメントシステムの継続的改善に関する事
- (2) RGF は、本規程を文書にして従業員に公示するとともに、顧客にも公示する。

1. 3. 4 内部の管理制度及び操作規程

- (1) RGF は、次の事項を含む内部の管理制度及び操作規程を制定し、実施する。
 - a) RGF における個人情報の取扱いに関する権限および責任の規定
 - b) 収集、告知及び同意取得に関する関連規定
 - c) 個人情報の保存、使用、加工、伝送に関する関連規定
 - d) 個人情報の提供、公開に関する関連規定
 - e) 個人情報の削除等に関する関連規定
 - f) 個人情報に関するリスク評価に関する規定
 - g) 苦情、相談および問い合わせへの対応に関する規定
 - h) 個人情報保護に関する教育の規定
 - i) 内部規程の違反に関する罰則の規定
 - j) 緊急事態への準備および対応に関する規定

1. 3. 5 責任および権限

1. 3. 5. 1 個人情報安全責任者（総経理）

- (1) 個人情報安全責任者（総経理）は、個人情報の適切な取扱いを事業運営上の重要課題と位置づけ、個人情報保護マネジメントシステムを効果的に実施するために、役割、責任および権限を定め、記録し、かつ、従業員及びその他の者に周知する。
- (2) 個人情報安全責任者（総経理）は、個人情報保護マネジメントシステムに関する自らの権限を、個人情報取扱責任者に委譲できる。

- (3) 個人情報安全責任者（総経理）は、個人情報保護マネジメントシステムの内容、「個人情報保護法」等の要求等を理解し、これに基づき RGF の個人情報の取扱いが適切に行われているかどうかについて、公平かつ客観的な立場で審査する能力のある者 1 名を指名する。
- (4) 個人情報安全責任者（総経理）は、従業員のなかから 1 名を情報システムセキュリティ担当者として指名する。

1. 3. 5. 2 個人情報取扱責任者

- (1) 個人情報取扱責任者は、個人情報保護マネジメントシステムの実施および運用に関する責任と権限を持ち、個人情報保護マネジメントシステムを実施し、個人情報安全責任者（総経理）にその運用状況を報告する。
- (2) 個人情報取扱責任者は、個人情報の安全管理が図られるよう、従業員等に対し必要かつ適切な監督を行う。
- (3) 個人情報取扱責任者は次の事項を検討し、決定または承認者に助言する権限を持つ。
 - a) 個人情報取扱いに関する規程等の制定および改廃
 - b) 個人情報取扱いに関する監査の実施時期や実施方法
 - c) 個人情報取扱いに関する教育・研修の実施時期や実施方法
 - d) 個人情報取扱規程の例外事由の適用
 - e) 新規の種類の個人情報の取得
- (4) 個人情報取扱責任者は次の事項に関する報告を受け、改善等の指示を行う。
 - a) 個人情報取扱いに関する運用実態および自主点検結果
 - b) 個人情報取扱いに関するあらゆる監査の結果
 - c) その他、個人情報取扱責任者が必要と認めた事項

1. 3. 5. 3 情報システムセキュリティ担当者

情報システムセキュリティ担当者は、個人情報保護マネジメントシステムにおける情報システムセキュリティの実施および運用に関する責任と権限を持つ。

1. 3. 6 個人情報の特定

RGF は、保有するすべての個人情報を特定し、特定した個人情報のリスクを把握し、必要な対策を講じる。

1. 3. 6. 1 個人情報の管理

情報安全管理室は、個人情報の取扱目的、取扱方法、個人情報の種類及び個人の権益への影響、存在する安全リスク等に基づき、個人情報に対して分類管理を実行し、暗号化、非識別化（個人情報に処理を施すことにより、更なる情報によらなければ特定の自然人を識別することができないようにするプロセスをいう）等の然るべき安全技術措置を講じて個人情報取扱行為が法律、行政法規の規定に合致することを確保し、かつ無権限のアクセス及び個人情報の漏洩、改竄、紛失を防止しなければならない。

1. 3. 7 リスク等の認識、分析および対策

- (1) 情報安全管理室は、一つの業務フロー図を作成し、個人情報の業務フロー図を取りまとめる。
- (2) 情報安全管理室は、個人情報の取得、利用、提供、保存および廃棄などその取扱いの各場面におけるリスクを調査し、取扱いシーン毎の想定リスク、安全対策、該当する規程及び残存リスクを業務フロー図とともに「リスク分析シート」に記載し、個人情報取扱責任者が承認する。
- (3) 個人情報の取扱いに関するリスクは、リスクの内容、発生した場合の被害の程度、実施されている対策の状況などによって、組織的、人的、技術的および物理的な側面より評価する。
- (4) 情報安全管理室は、把握された個人情報に関するリスクに対し、合理的な対策を講じる。
- (5) 情報安全管理室は、個人情報に関するリスクを毎年審査する。

1. 3. 8 個人情報の取扱いに関する事故への対応

- (1) RGF は、個人情報の漏洩、改竄、紛失が生じ、又は生じるおそれがあるとき等個人情報の安全に関わる事象（以下「事故」という。）に対する緊急対応策を制定し、かつ実施を手配する。
- (2) RGF は、1.3.8.1～1.3.8.3 における事故の特定および対応の手順に従い、直ちに改善措置を講じ、かつ個人情報保護職責履行部門及び個人に通知しなければならない。通知には次に掲げる事項を記載しなければならない。
 - a) 個人情報の漏洩、改竄、紛失が生じ、又は生じるおそれのある情報の種類、原因及び生じるおそれのある危害
 - b) RGF が講じた改善措置及び危害を軽減するために個人が講じうる措置
 - c) RGF の連絡先
- (3) RGF が措置を講じることによって情報の漏洩、改竄、紛失により生じる危害を有効に回避できる場合、個人情報取扱者は、個人に通知しないことができる。

1. 3. 8. 1 事故の把握と対応の決定

- (1) 事故の発生を認知した従業員等（認知の手段は、社内・外による報告、相談又はクレーム提起等を含む）は、事実をすみやかに情報安全管理室に報告し、情報安全管理室は個人情報取扱責任者および個人情報安全責任者（総経理）に報告する。
- (2) 個人情報取扱責任者は、迅速、的確な対応が可能な体制を構築することで情報の一元化を図り、被害拡大の防止の指示等を行う。
- (3) 個人情報取扱責任者からの指示は、通常業務に優先して取り組む。

1. 3. 8. 2 通知・公表

- (1) 個人情報取扱責任者の指示を受けた者は、事故発生的事实および漏洩、滅失または毀損が生じた個人情報の内容を本人にすみやかに通知し、または本人が容易に知り得る状態に置く。
- (2) 個人情報取扱責任者は、二次被害の防止、類似事案の発生回避などの観点から必要があるときは、事実関係、発生原因および対応策を可能な限りすみやかに公表する。
- (3) 個人情報取扱責任者は、事故に関して、個人情報保護職責履行部門から要求を受けた場合、当該要求に従って、措置を講じ、これを是正し、潜在的危険性を取り除くものとする。

1. 3. 8. 3 事故の対応実施

- (1) 従業員等が、社外によるクレーム又は問い合わせにより事故の発生を認知した場合、または、個人情報管理に関する社内のコンプライアンス問題を発見した場合、当該従業員等は上司に

報告したうえで、直ちに情報安全管理室に対して報告を行い、情報安全管理室は、「苦情、相談および問い合わせへの対応に関する規定」、「緊急事態への準備および対応に関する規定」に従って、当該社外の方にフィードバックを行う。または、社内の問題を解決することと情報管理体制を改善する。

1. 3. 8. 4 事後処理

- (1) 個人情報取扱責任者は、再発防止策を立案するとともに実行を指示する。
- (2) 個人情報取扱責任者は、再発防止策が実行されていることを確認し、再発防止策の効果を確保する。
- (3) 情報安全管理室は、事故の発生から事後処理までの一連の対応を記録し、必要に応じて関係者が参照できる状態で管理する。

第2章 個人情報の取得、利用および提供に関する措置

2. 1 利用目的の特定

- (1) 個人情報の取得にあたっては、明確かつ合理的な目的がなければならず、かつ取扱目的と直接関わりがなければならず、個人の権益に対する影響が最小の方法を採用しなければならず、取扱目的を実現するための最小範囲に限定し、度を超えて個人情報を収集してはならない。
- (2) 個人情報の取得にあたっては、公開かつ透明の原則に従い、個人情報取扱規則を公開し、取扱の目的、方法及び範囲を明示しなければならない。
- (3) 求職者情報は、RGF が職業紹介およびこれに関連するサービスを求職者に提供することを目的として取得する。
- (4) 取引先従業員情報は、RGF が職業紹介およびこれに関連するサービスを提供すること、ならびに取引先と RGF が良好な取引関係を構築することを目的として取得する。
- (5) 従業員情報は、RGF が従業員等の就業管理を適切に行うことを目的として取得する。

2. 2 適正な取得

個人情報の取得は、適法かつ公正な手段によって行う。

2. 3 機微な個人情報の取得、利用および提供の制限

機微な個人情報とは、一旦漏洩され、又は不法に使用されると、自然人の人格の尊厳が侵害を受け、又は人身、財産の安全が害されやすい個人情報であり、生体認証、宗教信仰、特定の身分、医療健康、金融口座、行動履歴等の情報、並びに 14 歳未満の未成年者の個人情報が含まれる。特定の目的及び十分な必要性があり、かつ厳格な保護措置を講じている場合に限り、機微な個人情報を扱うことができる。

- (1) 機微な個人情報を扱うにあたっては、本人の個別の同意を得なければならない。法令に機微な個人情報の取得にあたっては書面による同意を取得すべき旨が定められている場合は、その規定に従う。
- (2) 機微な個人情報を取り扱う場合、明確な方法及びわかりやすい言葉で、本人に対し、次の事項を事実のとおり、正確かつ完全に通知しなければならない。
 - (一) RGF の名称及び連絡先
 - (二) 個人情報の取扱目的、取扱方法、取り扱う個人情報の種類、保存期間
 - (三) 個人の権利行使の方法及び手続
 - (四) 法令に通知すべき旨が定められているその他の事項前項に定める事項に変更が生じた場合には、変更部分を本人に通知しなければならない。
- (3) 機微な個人情報を取り扱う場合、本人に対し、機微な個人情報を取り扱う必要性及び本人の権益に対する影響も告知しなければならない。但し、法律の規定に従い本人に対し告知しなくてよい場合はこの限りでない。
- (4) 14 歳未満の未成年者の個人情報の取扱にあたっては、未成年者の父母又はその他の後見人の同意を取得しなければならない。14 歳未満の未成年者の個人情報の取扱にあたっては、専用の個人情報取扱規則を制定しなければならない。

2. 4 個人情報の取扱に関する措置

- (1) 個人情報の取扱にあたっては、合法、正当、必要及び信義誠実の原則に従わなければならない。誤導、詐欺、脅迫等の方法により個人情報を取り扱ってはならない。
- (2) 個人情報の取扱にあたっては、他人の個人情報を不法に収集し、使用し、加工し、伝送してはならず、他人の個人情報を不法に売買し、提供し、又は公開してはならず、国の安全、公共の利益を害する個人情報取扱行為に従事してはならない。
- (3) 次のいずれかに該当する場合に限り、RGF は個人情報を取り扱うことができる。
 - a) 本人の同意を得ているとき
 - b) 本人を当事者の一方とする契約の締結、履行のために必要であるとき、又は法に従い制定された労働規則制度及び法に従い締結された集団契約に従い人材資源管理を実施するために必要であるとき
 - c) 法定の職責又は法定の義務の履行のために必要であるとき
 - d) 突発的な公衆衛生事象に対応するため、又は緊急の場合において自然人の生命健康及び財産の安全を保護するために必要であるとき
 - e) 公共の利益のためニュース報道や世論による監督等の行為を実施するにあたり、合理的な範囲内で個人情報を取り扱うとき
 - f) 本人が自ら公開した個人情報又はその他のすでに合法的に公開されている個人情報を法律の規定に従い合理的な範囲内で取り扱うとき
 - g) 法令に定めるその他の事由法律の関連規定に従い、個人情報を取り扱うにあたっては本人の同意を取得しなければならない。但し、前項 b) から g) に定める状況にあるときは、本人の同意を得る必要はない。

2. 5 個人情報公開に関する措置

RGFは、その取り扱う個人情報を公開してはならない。但し、個人の個別の同意を取得している場合はこの限りでない。

2. 6 個人情報の提供等に関する措置

- (1) RGFは、個人情報を第三者に提供する場合には、本人に対し、受領者の名称又は氏名、連絡先、取扱目的、取扱方法及び個人情報の種類を告知し、かつ本人の個別の同意を取得しなければならない。
- (2) RGFは、個人情報を第三者から受領する場合には、その取扱目的、取扱方法及び個人情報の種類等の範囲内において個人情報を取り扱わなければならない。当初の取扱目的、取扱方法を変更する場合、「個人情報保護法」の規定に従い、あらかじめ本人の同意を取得しなければならない。

2. 7 個人情報の域外提供に関する措置

- (1) RGFは、業務等の必要により、中国国外に個人情報を提供する必要が確実にある場合は、次に掲げるいずれかの条件を備えていなければならない。
 - a) 「個人情報保護法」第40条の規定に従い国のネットワーク安全情報部門が行う安全評価に合格すること
 - b) 国のネットワーク安全情報部門の規定に従い専門機構が行う個人情報保護に係る認証を受けること
 - c) 国のネットワーク安全情報部門が制定する標準契約に従い国外の受領者と契約を締結し、双方の権利及び義務を約定すること
 - d) 法律、行政法規又は国のネットワーク安全情報部門が定めるその他の条件
- (2) RGFは、国外受領者による個人情報取扱行為が本法に定める個人情報保護基準を満たすことを保障するため、必要な措置を講じなければならない。
- (3) RGFは、中国国外に個人情報を提供する場合、個人に対し、国外の受領者の名称又は氏名、連絡先、取扱目的、取扱方法、個人情報の種類及び個人が国外の受領者に対し本法に定める権利を行使する方法及び手続等の事項を告知し、かつ個人の個別の同意を取得しなければならない。

第3章 個人情報の適正管理

3. 1 正確性の確保

RGFは、個人情報の取扱にあたっては、個人情報の品質を保証しなければならず、個人情報

が不正確、不完全であることにより本人の権益に不利な影響がもたらされることを避けなければならない。

3. 2 安全性の確保

RGF は、その個人情報取扱行為について責任を負い、かつ必要な措置を講じて、取り扱う個人情報の安全を保障しなければならない。

3. 3 従業員等の責務

- (1) RGF は、従業員等に個人情報を取扱わせるに当たっては、当該個人情報の安全管理が図られるよう、当該従業員等に対し必要かつ適切な監督を行う。
- (2) RGF は、従業員等の入社および退職時に、在職期間中本規程を遵守し退職または契約終了後であっても個人情報を他に漏らさない旨の書面を本人に提出させる。
- (3) 個人情報の取得、利用または提供に従事する従業員等は、法令の規定または本規程もしくは個人情報安全責任者（総経理）及び個人情報取扱責任者が指示した事項に従い、個人情報の安全管理に十分な注意を払いつつその業務を行う。
- (4) 従業員等は、本規程などに違反する事実を知った場合や違反のおそれがあることを発見した場合は、個人情報安全責任者（総経理）及び個人情報取扱責任者にすみやかに報告する。

3. 4 個人情報の保存および廃棄

3. 4. 1 保存および安全管理

- (1) 個人情報は、その利用目的に応じて保存期間を定め保存する。個人情報の保存期間は、法律、行政法規に別段の定めがある場合を除き、取扱目的を実現するために必要な最も短い時間で行なければならない。
- (2) 個人情報を含む文書は机上などに放置してはならない。
- (3) 個人情報を含む電子ファイルをサーバに保存する場合、業務上必要な者だけがアクセス出来るよう、アクセス権の設定を行う。
- (4) 情報安全管理室が許可していないインターネット環境や多機能携帯端末、個人所有のパソコンや電子媒体などに個人情報を保存することは禁止する。

3. 5 情報システムセキュリティ

3. 5. 1 コンピュータ機器等の管理

- (1) オフィス外へ持ち出す可能性のあるパソコンにはハードディスク暗号化ソフトウェアをインストールする。
- (2) 離席時に情報の盗み見や不正な操作がなされることを防ぐ為、「パスワードで保護されたス

- クリーンセーバー機能」を5分以内に作動するように設定する。
- (3) 業務に必要なソフトウェアはインストールしてはならない。
 - (4) 情報安全管理室が許可していないコンピュータ機器（パソコン、ルータ、モデム等）の、当社コンピュータ機器・ネットワーク等への接続を禁止する。
 - (5) 標準パソコンは、情報安全管理室が許可した方法でネットワークに接続しなければならない。

3. 5. 2 情報システムの論理的保護

3. 5. 2. 1 認証

情報システムへのアクセス制御を実行するため、利用者には一意的な固有のアカウントとパスワードを与え管理する。

情報システムの利用形態や利用者の権限などに応じて、利用可能な情報を適切に制限、分離し、不正利用による被害の拡大等を抑止する。

3. 5. 2. 2 暗号の利用

重要な情報の機密性保護のため、必要に応じてデータや通信手段の暗号化を行う。

3. 5. 2. 3 セキュリティ監視と維持

- (1) 発行した全ての ID の利用ログ（ログインの成功／失敗、ログアウト、ログアウトが取れない場合はセッションタイムアウト）を取得し記録日から6ヵ月間保存する。
- (2) 不正利用やセキュリティ侵害を防ぐために、適切な監視を行う。また、セキュリティを維持するために必要な技術などを取得して、必要に応じてすみやかに適切な対応を行う。

3. 5. 2. 4 バックアップ

重要な情報やシステムについては、必要な範囲でファイル・データのバックアップを行い、適切な保存、管理を行う。

3. 5. 2. 5 ウィルスチェック

- (1) パソコンにはウィルス検知ソフトを導入しリアルタイムでのウィルスチェックを行う。電子メールの受信、外部 Web サイトの閲覧、FTP や HTTP 等によるファイル取得等、ファイルやデータを取得する場合には、自動的にそれらのファイル等に対してウィルスチェックを行う設定とする。
- (2) 標準パソコンは、システムインフラ管理部署の定めたスケジュールに従ってパターンファイルを更新し、情報安全管理室の指示に従いフルスキャンを実施する。

3. 5. 3 ネットワークの管理

- (1) 接続先ネットワークと自己の管理するネットワークとの間にファイアウォール（ファイアウォール機能を持つルータを含む）を設置・設定・ログ管理する。
- (2) RGF ネットワークへの接続口等を設置する場合、ネットワークの利用制限／接続口を施錠して利用制限を掛けるなど、不要な機器が接続出来ない対策を施す。
- (3) 外部からインターネットを経由して接続を行う場合、VPN 等を用いて認証及び盗聴・改ざん

対策を施す。

3. 5. 4 情報システムの廃棄

利用しなくなった情報システムを廃棄する場合には、廃棄物から情報が漏洩しないように、破壊や焼却などの物理的手段または情報を復元できない措置などの論理的手段により適切な消去を行う。

3. 6 個人情報の委託処理に関する措置

個人情報の取扱いを委託する場合、受託者と取扱委託の目的、期間、取扱方法、個人情報の種類、保護措置並びに双方の権利及び義務等を約定し、かつ受託者の個人情報取扱行為を監督しなければならない。

3. 7 合規性監査

RGF は、その個人情報の取扱における法律、行政法規遵守状況について定期的に合規性監査を行わなければならない。

第 4 章 個人情報に関する本人の権利

4. 1 個人情報取扱行為における個人の権利

4. 1. 1 知る権利と決定権

個人は、その個人情報の取扱について知る権利、決定権を有し、その個人情報を他人が取り扱うことを制限し、または拒絶する権利を有する。但し、法律、行政法規に別段の定めがある場合はこの限りでない。

4. 1. 2 閲覧、複製、移転

- (1) 個人は、RGF からその個人情報を閲覧し、複製する権利を有する。但し、「個人情報保護法」第 18 条第 1 項、第 35 条に定める事由がある場合はこの限りでない。
- (2) 個人がその個人情報の閲覧、複製を請求した場合、RGF は、遅滞なく提供しなければならない。

- (3) 個人がその指定する RGF への個人情報の移転を請求し、国のネットワーク安全情報部門の定める条件を満たしているときは、RGF は、移転手段を提供しなければならない。

4. 1. 3 訂正と補充

- (1) 個人は、その個人情報が不正確又は不完全であることを発見した場合、RGF に対し訂正、補充を請求する権利を有する。
- (2) 個人がその個人情報の訂正、補充を請求した場合、RGF は、その個人情報について事実確認を行い、かつ遅滞なく訂正し、補充しなければならない。

4. 1. 4 削除

次に掲げる事由のいずれかに該当する場合、RGF は、自主的に個人情報を削除しなければならないが、RGF が削除していないときは、個人は、削除を請求する権利を有する。

- a) 取扱目的が実現されたとき、実現不能であるとき、または取扱目的の実現のために必要ではなくなったとき
- b) RGF が製品もしくは役務の提供を停止するとき、または保存期間が満了したとき
- c) 個人が同意を撤回したとき
- d) RGF が法律、行政法規に違反し、または約定に違反して個人情報を取り扱ったとき
- e) 法律、行政法規に定めるその他の事由

法律、行政法規に定める保存期間が満了していない場合、又は個人情報の削除が技術的に実現困難である場合は、RGF は、保存及び必要な安全保護措置の実施以外の取扱を停止しなければならない。

4. 2 個人による権利行使

RGF は、個人による権利行使の申請の受理及び処理の手軽な仕組みを構築しなければならないが、個人による権利行使の請求を拒絶する場合には、理由を説明しなければならない。

第 5 章 個人情報の取扱いに関する教育・研修

5. 1 教育・研修の実施

- (1) RGF は、従業員等を対象に、個人情報の取扱いに関する安全教育・研修を定期的にも実施しなければならない。

- (2) RGF は、関連する教育・研修・試験評価計画を策定し、実施するものとする。
- (3) 情報安全管理室は、安全教育・研修・試験評価の実施結果を RGF の関連する担当者に報告し、業務の改善及び調整をする。

第 6 章 個人情報保護影響評価の実施・記録作成・保存

6. 1 個人情報保護影響評価の実施・記録作成

RGF は、次に掲げる事由のいずれかがあるときは、事前に個人情報保護影響評価を行い、かつ取扱状況について記録を取らなければならない。

- (1) 機微な個人情報の取扱
- (2) 個人情報を利用した自動化された意思決定
- (3) 個人情報の取扱の委託、その他の個人情報取扱者への個人情報の提供及び個人情報の公開
- (4) 個人情報の国外への提供
- (5) その他個人の権益に重大な影響を与える個人情報取扱行為

6. 2 個人情報影響評価の内容

個人情報影響評価には次に掲げる内容を含めなければならない。

- (1) 個人情報の取扱目的、取扱方法等が合法的、正当かつ必要なものであるか。
- (2) 個人の権益に対する影響及び安全リスク
- (3) 講じる保護措置が合法的かつ有効であるか、かつリスクの程度に見合ったものであるか。

6. 3 個人情報保護影響評価報告及び取扱状況の保存

個人情報保護影響評価報告及び取扱状況の記録は、少なくとも 3 年間保存しなければならない。

第 7 章 苦情、相談および問い合わせへの対応

7. 1 苦情、相談および問い合わせに関する受付窓口の設置

- (1) RGF は、個人情報の取扱いおよび個人情報保護マネジメントシステムに関する苦情、相談および問い合わせの受付窓口を設置し、顧客に対してホームページ上でその連絡先を公表する。

- (2) 受付窓口は情報安全管理室に設置し、苦情、相談および問い合わせに対してすみやかに回答する。
- (3) 苦情、相談および問い合わせの受付は、ウェブサイトのお問い合わせフォームにより行う。
- (4) 情報安全管理室以外で苦情、相談および問い合わせを受け付けた場合は、すみやかに情報安全管理室にその内容を報告し、回答内容および回答担当者/責任者を協議、決定した上で回答しなければならない。

7. 2 苦情、相談および問い合わせの内容の記録と報告

- (1) 情報安全管理室は、苦情、相談および問い合わせの内容と対応結果を記録し、保存する。
- (2) 情報安全管理室は、苦情、相談および問い合わせに関する記録を個人情報取扱責任者と個人情報安全責任者（総経理）に定期的に報告する。

7. 3 重大案件への対応

情報安全管理室は、苦情、相談および問い合わせの内容が重大であると判断したときは、ただちに個人情報取扱責任者に報告しなければならない。個人情報取扱責任者と関係者および個人情報安全責任者（総経理）を招集して協議し、対応を決定する。

第8章 その他

8. 1 罰則

省略（社内規定より処理する）

8. 2 規程の改廃

本規程の改廃は、個人情報取扱責任者が起案又は提案し、総経理が承認する。

8. 3 疑義取扱

本規程に定められた事項に疑義ある場合またはその取扱いについて定めのない場合は、その都度個人情報取扱責任者の意見に基づき、個人情報安全責任者（総経理）がこれを定めるものとする。

第9章 付則

本規程は、2021年11月1日から施行する。