別紙１「クマキャリ！熊本市キャリア相談所情報セキュリティについて」

公式LINEアカウント「クマキャリ！熊本市キャリア相談所」の情報セキュリティについては、下記のとおりとする。

１．情報セキュリティ

（１）サービスレベルの合意

下記のサービスレベルで合意する。

No.	種別	サービスレベル項目	規定内容	測定単位	サービスレベルの設定
1	可用性	稼働率	サービスを利用できる確率（（計画サービス時間－停止時間）÷計画サービス時間）	稼働率（%）	95%以上
2		目標復旧時間	障害発生後のサービス提供の再開に関して設定された目標時間	時間	1日後
3		目標復旧ポイント	障害発生後のサービス提供の再開に関して設定されたポイント	内容	障害発生時点の最新バックアップからの復旧とする
4		バックアップの保管方法	バックアップ内容（回数、復旧方法など）、データ保管場所／形式	内容	日次で、作業前後の差分のみバックアップし、週次でフルバックアップを取る。遠隔地のデータセンタにテープ形式保管。
5		復旧要件	災害発生時のシステム復旧／サポート体制について	内容	遠隔地のバックアップ用データセンタで保管している日次バックアップデータと予備システムへの切り替えを行う。
6	情報セキュリティ	情報セキュリティインシデントの対応について	情報セキュリティインシデント発生時の対処手順、責任分界、対処体制を記載する。	内容	発生から15分以内（基幹業務）、2時間以内（その他業務）に担当者から熊本市に通知し、協議の上で対応する。受託者の責めに帰すべき事由がない場合、受託者は責任を負わない。
7		情報セキュリティ対策について	脅威に対する情報セキュリティ対策（なりすまし、情報漏えい、情報の改ざん、否認防止、権限	内容	受託者が熊本市に対して、規定された情報セキュリティ対策の実施状況を月次で報告を行う。

			昇格への対応、サービス拒否・停止等）の実施状況やその他の契約の履行状況の確認方法		
8			情報セキュリティ対策の履行が不十分な場合の対処方法	内容	受託者は熊本市と改善について協議を行い、合意した改善策を実行する。
9	その他	変更時の対応について	外部サービス提供者による利用規約、各種設定が変更された場合の変更内容の確認方法や連絡方法	内容	変更の 10 日前に受託者から熊本市にメールで通知する。

（2）特記事項

ア　一般財団法人日本情報経済社会推進協会が認証する「プライバシーマーク」又は国際規格ＩＳＯ／ＩＥＣ２７００１の評価基準である「情報セキュリティマネジメントシステム（ＩＳＭＳ）適合性評価制度」認証の取得又は同等程度の水準を備えていること。

イ　日本の裁判管轄、法令が適用されること。海外への機密情報の流出リスクを考慮し、外部サービスを提供するリージョン（国・地域）を国内に指定すること。国内の外部サービスにおいて、利用者のデータが、海外に保存されないこと。

ウ　外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制について、公開資料や監査報告書（又は内部監査報告書・事業者の報告資料）の内容を確認する。

エ　外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、利用者の意図しない変更が加えられないための管理体制について、公開資料や監査報告書（又は内部監査報告書・事業者の報告資料）の内容を確認する。

オ　不正なアクセスを防止するためのアイディンティティ管理（ID のプロビジョニングから廃棄まで）とアクセス制御を実装すること。

カ　システム管理者等の特権アカウントが外部サービスに接続する際は、強化された認証技術（多様素認証等）を用いること。

キ　外部サービス利用者による外部サービスに影響を与える操作の特定と誤操作の抑制するために、手順書の作成や誤操作を認識可能なアラート等の実装を考慮すること。

ク　外部サービス上で構成される仮想マシンに対して、適切なセキュリティ対策（WAF）を行うこと。

ケ　適切な暗号アルゴリズム（CRYPTREC により安全性及び実装性能が確認された「電子政府推奨暗号リスト」）を用いた暗号化処理を行うこと。

コ　外部サービスの企画、要件の確認の段階から想定される脅威やリスクに対するセキュリティ対策を検討し、その検討結果を踏まえ、設計・開発におけるセキュリティ対策を行うこと。また、外部サービスで取得可能なログの種類、範囲等を確認し、必要となるログの取得機能を実装すること。

サ　外部サービス内における取得するログの時刻、タイムゾーンを統一すること。

シ　設計・設定時の誤りの防止の対応として、設計書や設定のレビューやクラウドサービ

スのフレームワークとの比較などを行うこと。
ス　セキュリティを保つための開発手順やフレームワーク等の情報を活用すること。
セ　外部サービス上に他ベンダが提供するソフトウェア等を導入する場合のそのソフトウェアの外部サービス上におけるライセンス規定を熊本市に報告すること。
ソ　外部サービス上に構成された情報システムと他の外部サービス利用者のネットワークやサブネット間等の異なるネットワーク間の通信（トラフィック）を監視すること。
タ　利用する外部サービス上の情報システムが利用するデータ容量や稼働性能（移植容易性）について、外部サービスの利用業務が継続できるよう考慮すること。
チ　外部サービスの利用に係る可用性（冗長構成や冗長回線等の実装）を考慮した設計とすること。
ツ　本業務で取り扱う情報は AWS 内に完結することとし、熊本市と受託者以外の第 3 者（LINE ヤフー株式会社、拠点に設定した店舗等）に個人情報等が漏えいすることが無いように管理すること。

（3）サポート
本市職員向けに操作のアドバイスや、より良い活用のためのアドバイス等のサポートを行うこと。

2．その他

（1）担保責任
受託者は、熊本市が本システムを利用する上で、プログラム上の瑕疵、バグ、エラー、脱落、欠陥、不一致やその他の原因により、利用したこと、または利用できなかったことにより生じた直接的、派生的、付随的または間接的損害(営業上の損害、業務の中断、営業情報の喪失などによる損害を含む)について、受託者の責めに帰すべき事由がない場合、責任は負わない。
（2）データの保存
ア　本システムの利用によって保存及び蓄積されたデータはすべて受託者の本システム用サーバに格納される。
イ　熊本市は、本契約が終了した場合、情報保護のため受託者が本システム用サーバ内に残存するデータを削除することに予め同意する。
（3）熊本市情報セキュリティ基本方針及び熊本市情報セキュリティ対策基準に記載された事項を遵守すること。また、熊本市 LINE サービス等の利用指針を遵守すること。
（4）本仕様書に定めのない事項については、委託者と協議の上、定めるものとする。