外部サービスの利用におけるセキュリティ要件

No	セキュリティ対策
1	受託者は情報セキュリティに関して十分な知識があること。
2	ライセンス違反等がないよう必要な数だけアカウントを準備すること。
3	利用する端末にセキュリティ対策（ユーザー認証・ウィルス対策・デバイス管理・Web フィルタリング等）を行っていること。
4	外部サービスを提供するシステム・利用する端末のリソースに不足がなく、将来の拡張性があること。
5	外部サービスで使用する時刻は、標準時刻と同期していること。
6	利用者の同時アクセスに耐えうるデータ通信速度を確認し、ネットワーク帯域を確保すること。
7	システムのレスポンス（応答時間）は許容範囲内であること。
8	ユーザが特別な知識を必要とせず、直感的に利用できるシンプルなデザインの画面や操作性となっていること。
9	データのバックアップ及びリストアができること。 バックアップのタイミング：毎日 保存世代：１週間分
10	インシデント等の検証に必要なログを提供できること。
11	OS やアプリケーション等のバージョンアップや設定変更、パッチ適用、脆弱性診断等を行い、実施状況を報告すること。
12	サービス終了時に保存データ（事業者の複製データも含む）を消去する際は、実効性を確保でき、データが復元不可能となる処置を講じること。
13	サービス終了時は利用者アカウントや管理者アカウント等を削除できること。
14	システムを事業者が構築する場合、事業者内において適切なセキュリティ管理体制（職員の資格取得や研修等）がとられていること。
15	重要な操作（仮想化されたデバイスのインストールや変更・削除、バックアップ・リストア、サービス終了時など）に関して、手順が文書化されていること。
16	システムを事業者が構築する場合、管理者等のアカウントは適切に管理（パスワード管理や多要素認証、アクセス権限、終了時の削除など）されていること。
17	事業者または区がインシデントを検知した際、区 CSIRT への連絡・報告体制が取れていること。
18	サービスのサポート体制や窓口、受付時間がサービス利用において十分なものになっていること。
19	情報の盗聴、改ざん等を防止するため、通信の暗号化がされていること。
20	盗難・改ざん等の防止のため、保存されたデータは暗号化されていること。
21	不必要なアクセスがされないよう、情報資産・機能に対して、各利用者に必要最低限のアクセス権のみ付与すること。
22	ID/PW による認証を行うこと。
23	ID/PW による認証に加え、メール認証または認証アプリを用いた二要素認証が可能であること。