W．その他サービス業（エステティックサロン）　W 社

事業概要	エステティックサロン運営		
従業員数	非公開	プライバシーマーク取得	なし
保有個人データ件数	非公開		

１．個人情報に関する概要

（１）保有する個人情報の件数、種類、利用目的

・個人情報の保有件数については非公開である。

・個人情報としては、氏名、住所、電話番号のほかに、エステティックサービスに必要な情報も取得している。

（２）個人情報保護担当部署

・個人情報保護担当部署(兼務)が設置されている。

（３）個人情報保護管理者の有無・位置づけ

・取締役が個人情報保護管理者として位置づけられている。

（４）認証取得の有無（時期)、認証の種類、その認証を取得した理由・効果

・認証は取得していない。

（５）個人情報保護に向けた取組経緯

・平成 15 年 8 月に「情報セキュリティ規程」を策定し、施行した。

・平成 16 年 8 月に個人情報保護に関する社内プロジェクトを発足し洗い出しを実施した。

・平成 17 年 3 月にサロン責任者及び本社全従業者に研修を実施した。

・平成 17 年 4 月より「個人情報保護管理規程」を施行。委託先に対する契約更新時に秘密保持契約の締結を推進している。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・特になし

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・プライバシーポリシー等は、ガイドライン、法律、書籍等を参考にコンサルタントの意見も聞いて作成した。

・個人情報保護の社内担当は 3 名（管理者を含む）である。個人情報保護の専任ではなく、他の仕事との兼務で行っている。

・規程についても定期的に見直す方向性で検討している。（平成 19 年はなし）

（２）個人情報の取得

・利用者は店舗に訪問し個人情報を会員となる為に登録する。

・利用者は広告媒体を見て電話又は WEB を通じて予約する。この際、個人情報を取得する。詳細な個人情報は来店時に取得し、紙媒体に記載する。

（３）個人情報の利用（第三者提供を含む）

（個人情報を識別できないようにした後にマーケティング分析に使用）

・プライバシーポリシー等では「個人情報を識別できない形式でのマーケティング情報収集及び商品の研究開発」のため個人情報を利用するとしている。分析には主に郵便番号を利用し、電話番号の市外局番は、携帯電話の登録が多いため利用していない。

（４）個人情報の管理

①情報の管理体制

（機微な個人情報は紙媒体でのみ管理し、大量漏えいを防止している）

・店舗において、利用者の個人情報をすべて紙媒体で管理している。店舗ごとに鍵のかかるロッカーに保管し、ロッカーは帰宅時に施錠している。サロン責任者が施錠の責任者となり、紙情報は、サロン責任者の指示がなければ持ち出せない規則となっている。

・本社においては、社外との回線を一箇所に絞っている。ファイヤーウォールや外向けの電子メールサーバは本社にあり、出入口を 1 つにすることで情報の流出入を管理している。

・本社ではデスクトップ PC をメインで使っている。デスクトップ PC には書き込みのできる CD ドライブは付けていない。

・ログインには ID、パスワードが必要である。部署ごとの共有サーバについても ID、パスワードが必要である。

・本社内はオンラインでつながっている。本社と各営業拠点は VPN（閉域網）でつながっている。

・個人情報のデータが保存されているのは、汎用機であるため、個人のパソコンへのデータのダウンロードはできない。
・ファイル共有ソフト（Winny 等）の使用は禁止している。資産管理ソフトをすべてのパソコンに入れており、起動チェックを行っている。
・電子メールの利用についてはアクセスログをとっている。容量制限をしており、大量にデータが外部に流出しないようにしている。
・本社内デスクトップＰＣは、各部署長が許可した場合に限り管理された暗号化ＵＳＢにのみ複写できるようにした（その他の媒体は原則不可とした）。（平成 20 年 6 月より）

②従業者への教育方法

・社内への周知徹底については、平成 17 年 3 月の法律施行にあわせて、本社から出向いて、サロン責任者（各店舗の責任者）教育と確認を行った。また本社の全従業者も対象に教育と確認を行った。
・サロン責任者には、「マニュアル」を配布し店舗において教育するよう徹底している。
・機微情報を扱っているので、情報の重要性は法施行前から教育している。また毎月の会合でも随時教育をしている。
・平成 18 年 11 月にセキュリティ週間を定め、本社各部署及びサロン責任者に対して研修と実施状況の確認を行った。以降、毎年 11 月に実施状況の確認を行っている。

③盗難対策

・店舗において機微情報は紙媒体でのみ管理されている。データ化はされない。紙媒体のため、隠れて大量に持ち出すことはできない。
・本社にあるデスクトップ PC の本体にセキュリティワイヤーをつけ、動かないようにしている。

④ノート PC の安全対策

・外回りの営業職はいないので、ノート PC は必要最低限にしている。ノート PC には USB セキュリティキーを利用している。ログイン時に USB キーを接続し、ID、パスワードを入力してはじめて立ち上がるようになっている。HDD の暗号化はしていない。

⑤外部委託先管理

・外部への提供はしない。
・書類の保管は、プライバシーマーク取得の外部業者を利用している。
・外部から個人情報を入手し、ダイレクトメール等を出すということはない。
・個人情報は、関連会社（共同利用会社）に必要な部分のみデータを提供する場合がある。

・関連会社においても本社と同一の管理基準を適用している。
・共同利用について利用者からの問合せや指摘は特にない。

⑥日常点検・確認の方策

・一般的な取組をしている。

⑦初歩的ミスの防止策

（FAX の誤送信防止のため、広域内線番号サービスを利用）

・紙情報の店舗間の移動には FAX を利用する場合もある。店舗間の通話網は NTT の広域内線番号サービス「メンバーズネット」を利用しており、内線番号で FAX 送信が可能である。社外へ間違って送ることはない。

（５）個人情報の消去・破棄

・プライバシーポリシー等の「開示・訂正・利用停止」の中で、「最終のご利用から相当期間を経過したお客様の情報に関しましては対応できない場合があります」としていて終了分を定期的に消去している。この記載に関する問い合わせは来ていない。
・ハードディスク・CD-ROM 等のディスクはセキュリティの観点から、破砕処理している。

（６）個人情報の監査

・外部のセキュリティ専門会社に依頼することについて検討中である。

（７）苦情処理・顧客対応

・問合せに対しては本社に「お客様相談室」を設け対応している。
・開示請求については、本人限定受取書留の費用を設定している。
・開示請求は当初想定していたよりも少なかった。

（８）事故発生時の対応

・漏えい、き損事故発生時への取組としては、保険加入と、連絡体制の整備がある。
・各部署には事故発生時のマニュアルを配布している。
・事故が発生した場合には、担当所属長又は部署の個人情報担当者へ連絡がなされ、委員会が招集される。代表取締役が対応委員長となっている。

以　上