

21 世紀型企业への転換を図る

■ 情報管理の実効性を向上させるためには ？！

～ 日頃の動機づけと習慣化 ～

つい、うっかり… ？！

現代社会において、インターネットや電子メール、大容量メモリーなどは、多くの職場において日常的に使用され、業務の効率的な遂行には欠かせないツールとなっています。

しかし、便利な反面で問題となりそうなのが、社員の独断利用や、それに伴う顧客情報・営業機密等の情報漏洩です。「自宅のパソコンで会社のメールをチェックしています…」「データを持ち帰って、自宅で作業しています…」など、幸いにも現実的な問題となっていないような、個人の軽はずみな行動が、いつか大きな問題にならないとは限りません。

企業では、さまざまな情報漏洩対策、退職後の守秘義務や競業避止、インターネットや電子メールの利用管理、記憶媒体の管理などを行っていますが、業務上の支障を考えると、まだまだ“社員の良心”に頼っているところが多いように思います。

関連する規程には「懲戒処分」と定義しながらも、データの置き忘れや盗難、メール誤送信といった“うっかりミス”を表面沙汰になっていないからと「いつもまじめにやっているから…」安易に許容されていないでしょうか。

まずは、社員一人ひとりが情報管理の必要性和機密保持の重要性をしっかりと理解し、過失による「事故や事件を起こさせない」という心構えをもてるようにすることが先決です。



会社の情報がSNSに… ！！

社員が私的生活上でSNS（ソーシャル・ネットワーキング・サービス）を利用することを企業が禁止することはできません。また、監視することは、プライバシー保護の観点からも、当然、好ましいことではないとされています。

ある報道では、企業や上司の干渉に対し、“ソーハラ”（ソーシャル・ハラスメントの略？）という言葉が使用されることもあるようです。しかし、このような私的なサイトで、会社や上司の悪口を書かれたり、営業上の機密情報を書かれたりすると大変なことになってしまいます。

“社員の良心”に頼り過ぎていると、このような事態が発生した場合に、後手後手の対応となり、後から「企業秩序を遵守する義務」と指導・教育しても、問題がこじれるばかりです。

企業が先行してリスクを予測し、先に手を打っておけば、“社員の良心”をそれなりに活かすことができ、万が一の際には、明文化した規定や運用マニュアルにより、正当な懲戒を行うことが可能となります。



Blog

情報は経営資源 ！

かつての高度経済成長期には、「人・物・金」が経営資源でしたが、現在では、これに「時間・情報」を加えて資源と位置付けることが当たり前となっています。

企業における多くの情報資源は、コンピュータ内部、各種記録媒体、紙、または人の記憶や知識など、さまざまな形態となり企業のあちこちに存在し、その価値がますます高まっているといえます。

そのような環境だからこそ、情報資源の管理を企業の情報システムに携わる担当者だけに任せるのではなく、全社的に取り組む必要があります。

情報セキュリティに関する事故、または法令違反などを発生させてしまうと、企業が深刻なダメージを受けてしまうことになります。



社会的信用低下

ブランドイメージの失墜、マーケットシェア低下、風評、株価暴落



行政指導

業務停止、免許剥奪、刑事責任、損害賠償責任



社内モラル低下

従業員の不安・不満

対策費用増大

見舞金・謝罪費、情報システムの改善費用

売上の減少

顧客からの取引停止、営業機会の損失

情報管理のポイントは ？！

企業の情報資源を安全に維持するためには、つぎの３つの切り口により、情報を管理運用することが考えられます。

◆ 機密性の確保

正当な権利を持った人だけが情報資源を使用できる状態にしておく。

⇒ 情報漏えい防止、アクセス権の設定などの対策

◆ 完全性の確保

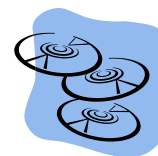
正当な権利を持たない人に情報資源が変更されていないことをチェックする。

⇒ 改ざん防止、検出などの対策

◆ 利便性の確保

情報資産を必要なときに使用できるようにする。

⇒ 電源対策、システムの二重化などの対策



労使トラブル業種別診断サービス ⇒ <http://www.iwaki-pmo.co.jp>

身近なところから始めましょう… !!

抽象的な内容の規程を作成するよりも、職場のルールとして以下のことを徹底してみましょう。

このことにより、社員一人ひとりが情報管理の必要性和重要性を認識するきっかけとなり、社員相互が牽制、注意しあいながら、自社のセキュリティに自信を持ち、少なくとも“うっかり”がなくなるような緊張感を持てるようになるものと思います。



● 身のまわりの情報漏えい対策 その①

常に、机の上の整理整頓を指導しましょう。美観を損ねる、という理由ではなく、機密情報を印刷した書類や媒体などを、他人の目に付く場所に放置しないようにしたり、情報の紛失を防いだりするために必要なことであることを繰り返し教育しましょう。

● 身のまわりの情報漏えい対策 その②

パソコンから離れる場合には、ディスプレイに情報が表示されないようにして、他人が容易に操作できないような処置を指導しましょう。

システムからログオフする、画面のロックを行う（パスワード付きスクリーンセ이버など）を利用し、機密情報を表示したまま席を立ち、他人に盗み見されたり、情報を改ざんされたりするなどの事故を防ぐための重要な処置となります。

● 身のまわりの情報漏えい対策 その③

退社時は確実に電源を落とし、他人に使われないようにする

メンテナンスや修理などで社外の業者へ一時的にパソコンを預ける場合は、機密情報データは別途記録媒体に保存して、ハードディスクから完全に消去しておくなどの対策を実行します。

● 身のまわりの情報漏えい対策 その④

DVD、USB メモリー、SD カードの記録媒体の管理については、廃棄の際に媒体を初期化したうえで、破碎してから廃棄する、管理者の許可なく、自宅へ持ち帰るなど社外に持ち出さない、私用の記録媒体は持ち込ませない、というルールを徹底します。

● 身のまわりの情報漏えい対策 その⑤

機密情報を印刷した用紙は、プリンタ、FAX、コピーなどで、裏紙として再利用しない。

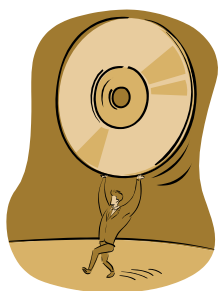
機密情報を印刷した場合は、すみやかに文書を自席に持ち帰るようにする。

機密情報が印刷された用紙を廃棄する場合、細かく裁断し、鍵のかかるゴミ箱に入れ、溶解業者へ処理を依頼する、などを徹底します。

以上のような対策は、情報セキュリティ管理規程などでみられるところですが、「実際に何をどうすればよいのか？」というところまでは記載されていないことが多いようです。

いいかえれば、「とりあえず作成した」、取引先評価における「規程のあり・なし」的なニーズにより作成しているだけで、実際にはあまり機能していないということに他なりません。

「何かあってからでは遅い！」これを起点とした実効性のある規程かどうか、万が一、違反した場合の処分をどうするのか、そして確実に処分できたのかどうか、このあたりが情報管理の実効性を向上するヒントになるのではないかと思います。



労働基準監督署への是正報告対応 ⇒ フリーダイヤル 0120-81-4864