BÀI 4

Bí mật kinh doanh

BÀI 4. Bí mật kinh doanh[1]

MỤC LỤC

GIỚI THIỆU CHUNG

Trong môi trường kinh doanh cạnh tranh khốc liệt, để đáp ứng nhu cầu và mong muốn mới ngày càng gia tăng của khách hàng hiện tại cũng như khách hàng tiềm năng, cần phải tạo ra các loại hàng hóa và dịch vụ mới hoặc cải tiến. Đối với một doanh nghiệp đang hoạt động hay một doanh nghiệp mới, muốn tồn tại, phát triển và đứng vững trong môi trường này, cần phải có đủ năng lực tự tạo ra hay tiếp nhận được các thông tin hữu ích cần thiết để tạo ra và cung cấp các hàng hóa và dịch vụ mới hoặc cải tiến ra thị trường. Những thông tin hữu ích như vậy chính là "bí mật kinh doanh" (hay còn được gọi là "bí mật thương mại"). Các đối thủ cạnh tranh thường tìm ra cách thức để tiếp cận những thông tin này theo cách dễ dàng, chẳng hạn như mua chuộc hay chỉ là

[1] Trong Bài này, thuật ngữ "bí mật kinh doanh" và "bí mật thương mại được hiểu như hau, và đôi khi được sử dụng thay thế cho nhau.

thuê lại các nhân viên chủ chốt của bạn – những người đã tạo ra hoặc được phép tiếp cận những thông tin bí mật và hữu ích mà đang mang lại lợi thế cạnh tranh cho doanh nghiệp của bạn. Để ngăn chặn sự suy giảm hay mất đi lợi thế cạnh tranh do những thông tin này đem lại, một công ty thành công phải bảo vệ tài sản hay thông tin bí mật của mình.

MỤC TIÊU CỦA BÀI HỌC

1. Giúp bạn hiểu được bản chất của bí mật kinh doanh, lý do bảo hộ chúng và các thách thức trong thực tế trong việc xác định và bảo hộ chúng.

2. Giúp bạn hiểu được cách thức xây dựng một chương trình quản lý bí mật kinh doanh có hiệu quả.

3. Giúp bạn hiểu được thế nào là sử dụng trái phép bí mật kinh doanh và cách thức ngăn chặn việc sử dụng trái phép này.

4. Giúp bạn hiểu được cách thức tiến hành các biện pháp thích hợp khác nhau để ngăn chặn hành vi xâm phạm bí mật kinh doanh.

5. Giúp bạn hiểu được lý do và cách thức tiến hành kiểm toán bí mật kinh doanh.

NỘI DUNG 1: Những vấn đề cơ bản về bí mật kinh doanh

1. Định nghĩa bí mật kinh doanh

Bí mật kinh doanh được định nghĩa là thông tin bất kỳ mà:

(1) Nói chung không được biết trong cộng đồng doanh nghiệp có liên quan hoặc với công chúng;

(2) Tạo ra những lợi ích kinh tế cho chủ sở hữu nó. Lợi ích này phải xuất phát từ việc thông tin đó nói chung không được biết, chứ không chỉ bởi giá trị của thông tin đó; và

(3) Cần có những nỗ lực cần thiết để duy trì bí mật này.

Một bí mật kinh doanh tiếp tục được duy trì miễn là thông tin đó tiếp tục được giữ kín.

Những thông tin bị bộc lộ một cách dễ dàng và hoàn toàn thông qua nghiên cứu đơn thuần các mặt hàng trên thị trường thì không thể là bí mật kinh doanh.

Tìm hiểu thêm: Lý do bảo vệ bí mật kinh doanh

1. Pháp luật về bí mật kinh doanh muốn duy trì và khuyến thích những chuẩn mực đạo đức và sự công bằng trong thương mại
2. Mục đích chính của pháp luật về bí mật kinh doanh là tạo ra động lực cho các doanh nghiệp sáng tạo bằng cách bảo vệ thời gian và nguồn vốn đáng kể đã được đầu tư vào việc phát triển những sáng tạo mang lại lợi thế cạnh tranh, cả về mặt kỹ thuật và thương mại, đặc biệt là những sáng tạo không được cấp bằng độc quyền sáng chế hoặc chưa đủ điều kiện để được cấp bằng độc quyền sáng chế.
3. Nếu không được bảo hộ bởi pháp luật về bí mật kinh doanh thì những đối thủ cạnh tranh của doanh nghiệp đó có thể sử dụng những sáng tạo này mà không phải gánh chịu bất kỳ phí tổn cũng như rủi ro nào trong quá trình nghiên cứu và phát triển những sáng tạo này.

Tham khảo thêm 1-1: Công thức của Coca-Cola

Có lẽ đây là "bí mật kinh doanh được giữ gìn cẩn trọng nhất trên thế giới."

Quy trình để bảo vệ công thức của Coca-cola (còn được biết đến với cái tên "Hàng hoá 7X") theo lời của một Phó Chủ tịch cấp cao và Cố vấn trưởng cho Coca-Cola tại một phiên tòa, như sau:

Các tài liệu dạng giấy mô tả công thức bí mật được giữ trong kho bảo đảm tại Ngân hàng Tín thác ở Atlanta, và kho này chỉ có thể được mở khi có một Nghị quyết của Ban Giám đốc Công ty. Chính sách của Công ty là vào bất cứ thời điểm nào cũng chỉ có hai người trong Công ty biết được công thức này, và chỉ những người đó mới có thể giám sát việc chuẩn bị Hàng hóa 7X trên thực tế.

Công ty cũng từ chối công bố danh tính của những người này và không cho phép những người này ở cùng bay trên một chuyến bay. Các biện pháp phòng ngừa tương tự cũng được áp dụng đối với các công thức bí mật của các loại nước uống Cola khác của Công ty như: Coke dành cho người ăn kiêng, Coke không chứa cafein dành cho người ăn kiêng, TAB, TAB không có chứa cafein và Coca-Cola không chứa cafein.

2. Loại thông tin mà có thể được bảo hộ làm bí mật kinh doanh

Hầu như bất kỳ loại thông tin nào cũng có thể là bí mật kinh doanh:

(1) Bí mật kinh doanh có thể bao gồm thông tin liên quan đến một công thức, mẫu hàng, thiết bị hoặc tập hợp các loại thông tin khác mà được sử dụng trong một thời gian nhất định trong một doanh nghiệp.

(2) Thông thường, bí mật kinh doanh là thông tin kỹ thuật dùng trong quá trình sản xuất hàng hoá.

(3) Bí mật kinh doanh có thể liên quan đến chiến lược tiếp thị, xuất khẩu hoặc bán hàng, hay phương pháp lưu trữ tài liệu hoặc các quy trình và thủ tục quản lý kinh doanh, kể cả phần mềm dùng cho các hoạt động kinh doanh.

Các ví dụ khác về bí mật kinh doanh tiềm năng có thể bao gồm thông tin kỹ thuật, khoa học và tài chính, như kế hoạch kinh doanh, quy trình kinh doanh, danh sách khách hàng chủ chốt, danh sách nhà cung cấp đáng tin cậy hoặc nhà cung cấp đặc biệt, bản mô tả đặc điểm kỹ thuật của sản phẩm, tính năng của sản phẩm, giá mua nguyên vật liệu thô, dữ liệu thử nghiệm, hình vẽ hoặc hình vẽ phác thảo kỹ thuật, thông số kỹ thuật chế tạo, công thức nấu ăn độc quyền, công thức tính toán, nội dung của sổ ghi chép trong phòng thí nghiệm, cơ cấu tiền lương của công ty, giá sản phẩm và mức chi cho hoạt động quảng cáo, mã nguồn, mã máy, cơ sở dữ liệu và tập hợp dữ liệu điện tử, hợp đồng chứa các chi tiết về ràng buộc thị trường, tài liệu quảng cáo hay tiếp thị đang được xây dựng.

Tham khảo thêm 1-2: Những thách thức và hạn chế của việc bảo hộ bí mật kinh doanh

Bí mật kinh doanh không thể được bảo hộ để chống lại việc tìm ra thông tin theo cách công bằng và trung thực, như một sáng chế độc lập hoặc kỹ thuật phân tích ngược.

Nếu một người không có quyền tiếp cận một cách hợp pháp những thông tin bí mật kinh doanh, nhưng lại giải mã được các thông tin đó mà không sử dụng bất kỳ phương tiện bất hợp pháp nào như sử dụng kỹ thuật phân tích ngược hay sáng chế độc lập, thì người đó không thể bị ngăn cấm sử dụng thông tin đã được tìm ra. Trong những trường hợp như vậy, chủ sở hữu bí mật kinh doanh không thể thực hiện bất kỳ hành động pháp lý chống lại người này.

Ưu điểm của việc bảo hộ bí mật kinh doanh:

1. Bảo hộ mật kinh doanh không mất chi phí đăng ký;

2. Bảo hộ bí mật kinh doanh không yêu cầu công bố thông tin hoặc thủ tục đăng

ký;

3. Bảo hộ bí mật kinh doanh vô hạn;

4. Bí mật kinh doanh có hiệu lực ngay lập tức.

Đối với các sáng chế có khả năng được cấp bằng độc quyền, thì nhược điểm của việc bảo hộ sáng chế đó dưới hình thức bí mật kinh doanh là:

1. Những bí mật có trong sản phẩm sáng tạo có thể bị tìm ra thông qua "kỹ thuật phân tích ngược" và được sử dụng một cách hợp pháp.
2. Bảo hộ theo hình thức bí mật kinh doanh chỉ bảo vệ bạn chống lại việc có được, sử dụng hoặc bộc lộ thông tin bí mật một cách trái phép.
3. Bí mật kinh doanh rất khó thực thi, vì mức độ bảo hộ được cho là yếu hơn so với bằng độc quyền sáng chế.
4. Một người có thể đăng ký bảo hộ sáng chế đối với bí mật kinh doanh của người khác nếu người đó tìm ra sáng chế tương tự với bí mật kinh doanh này bằng các biện pháp hợp pháp.

NỘI DUNG 2: Chương trình quản lý bí mật kinh doanh

1. 10 bước xây dựng Chương trình quản lý bí mật kinh doanh

(1) Xây dựng một hệ thống phù hợp để nhận biết các bí mật kinh doanh

Việc nhận biết và phân loại các bí mật kinh doanh là một điều kiện tiên quyết để bắt đầu một Chương trình bảo vệ bí mật kinh doanh. Các bước thực hiện để bảo vệ bí mật kinh doanh của bạn phải được quyết định bởi bản chất của chính những bí mật đó.

a. Các câu hỏi cơ bản cần được đặt ra là:
   - Những thông tin nào có thể làm tổn hại công việc kinh doanh của bạn nếu đối thủ cạnh tranh có được thông tin này?
   - Mức độ tổn hại sẽ đến đâu?

b. Các câu hỏi có liên quan cần được đặt ra là:
   - Bạn có nhân viên chuyên trách để lưu trữ, bảo mật dữ liệu hoặc bảo quản các bí mật kinh doanh hay không?

Hãy lập một danh mục bằng văn bản về những thông tin sẽ được bảo vệ và phân chúng thành các nhóm khác nhau, tùy thuộc vào giá trị của nó đối với doanh nghiệp và các biện pháp bảo vệ cần được áp dụng đối với từng thông tin.

(2) Xây dựng chính sách an ninh thông tin, bao gồm chính sách bảo vệ bí mật kinh doanh

Chính sách an ninh thông tin bao gồm các hệ thống và quy trình được thiết kế nhằm bảo vệ các tài sản thông tin nhằm tránh bộc lộ những thông tin đó cho bất kỳ người hoặc tổ chức nào mà không có quyền truy cập thông tin đó, đặc biệt là thông tin được coi là nhạy cảm, độc quyền, bí mật hoặc được phân loại (như trong lĩnh vực quốc phòng).

a. Điều quan trọng là phải có chính sách bảo vệ an ninh thông tin hoặc bí mật kinh doanh bằng văn bản. Chính sách bằng văn bản cần quy định rõ về tất cả các vấn đề sau:
   - Lý do và cách thức phải bảo vệ thông tin;
   - Cách thức bộc lộ và chia sẻ thông tin nội bộ hoặc với bên ngoài;
   - Cam kết của doanh nghiệp để bảo vệ bí mật kinh doanh bởi chính sách này sẽ đóng vai trò quan trọng trong trường hợp không thể tránh khỏi tranh chấp.
b. An ninh thông tin có thể được thực hiện ở các cấp độ khác nhau như sau:
   - Kiểm soát thủ công;
   - Kiểm soát hành chính;
   - Kiểm soát kỹ thuật.

(3) Giáo dục tất cả nhân viên về các vấn đề liên quan đến an ninh thông tin

a. Luôn luôn thuê nhân viên vì họ có kiến thức và kỹ năng phù hợp chứ không phải là vì họ đã tiếp cận được bí mật kinh doanh của doanh nghiệp cũ.
b. Tất cả các nhân viên phải biết rằng họ đã hiểu chính sách và rằng họ đồng ý tuân thủ chính sách đó. Nhắc lại chính sách đó một cách định kì.
c. Tránh thuê người bị ràng buộc bởi một thỏa thuận không cạnh tranh. Nếu buộc phải làm việc này thì hãy xin tư vấn của luật sư độc lập và có chuyên môn phù hợp.
d. Tránh việc phải bồi thường cho một nhân viên mới – người mà đang bị ràng buộc bởi một hợp đồng không cạnh tranh với doanh nghiệp cũ, vì nếu làm như vậy sẽ làm tăng nghi ngờ về những hành vi sai trái và có thể làm phát sinh nghĩa vụ tài chính nếu việc làm sai trái đó bị chứng minh trước tòa.
e. Nhắc nhở nhân viên của bạn không được bộc lộ bí mật kinh doanh cho cá nhân hoặc tổ chức không được phép biết và tuân thủ các thủ tục an ninh bằng cách thông báo, các bản ghi nhớ, e-mail, bản tin, v.v..

f. Việc thuê nhiều hơn một nhân viên của đối thủ cạnh tranh sẽ làm gia tăng nghi ngờ về hành vi sai trái, do đó nên tránh làm việc này.

(4) Tầm quan trọng của việc cẩn trọng khi thuê nhân viên của đối thủ cạnh tranh

a. Giáo dục và đào tạo nhân viên về chính sách an ninh thông tin.
b. Biến mọi nhân viên thành nhân viên bảo mật.
c. Mỗi nhân viên phải góp phần tạo ra một môi trường an toàn.
d. Ngăn chặn việc bộc lộ vô ý có thể xảy ra do sự thiếu hiểu biết.
e. Các nhân viên cần được huấn luyện để nhận biết và bảo vệ bí mật kinh doanh đúng cách.

<Đối với nhân viên thôi việc >

Hãy làm cho nhân viên thôi việc của công ty nhận thức được nghĩa vụ của họ đối với công ty cũ bằng cách thực hiện các cuộc nói chuyện trước khi họ ra đi, trong đó tập trung vào các vấn đề liên quan đến bảo mật, bí mật kinh doanh, v.v..

Nếu cần thiết hoặc mong muốn, công ty có thể yêu cầu họ ký thỏa thuận bảo mật mới hoặc cập nhật. Bạn cũng có thể viết thư cho doanh nghiệp mới của họ thông báo về các vấn đề liên quan đến bí mật kinh doanh để nhân viên nghỉ việc đó không bị chủ doanh nghiệp mới phân công vào các dự án hoặc hoạt động mà không hoặc khó có thể tránh khỏi việc bộc lộ bí mật kinh doanh của bạn.

(5) Đưa các giới hạn hợp lý vào tất cả các hợp đồng

Việc ký kết hợp đồng bảo mật hay không tiết lộ phù hợp với các nhân viên, nhà cung cấp, nhà thầu, đối tác kinh doanh có vai trò to lớn trong việc giữ thông tin không bị tiết lộ cho đối thủ cạnh tranh.

a. Các điều khoản không phân tích

Hãy đưa các điều khoản không phân tích vào hợp đồng chuyển giao bí mật kinh doanh để Bên kia chấp nhận không phân tích tài liệu hoặc mẫu bất kỳ được cung cấp theo hợp đồng nhằm mục đích xác định các thành phần, đặc tính, đặc điểm hoặc chi tiết kỹ thuật, trừ khi được phép bằng văn bản của người đại diện được ủy quyền hợp pháp của công ty bạn.

b. Các điều khoản không tấn công, không tuyển dụng hoặc không xúi giục

Điều khoản về không tấn công, không tuyển dụng hoặc không xúi giục trong hợp đồng lao động sẽ cấm nhân viên nghỉ việc gạ gẫm đồng nghiệp rời khỏi công ty cùng người đó để làm việc cho một doanh nghiệp khác hoặc thành lập một doanh nghiệp cạnh tranh mới.

(6) Hạn chế tiếp cận hồ sơ giấy tờ

Để ngăn chặn việc tiếp cận trái phép hồ sơ bảo mật, nhạy cảm, bí mật hoặc chỉ hạn chế đối với những nhân viên được phép được xem chúng khi cần biết.

Điều này có thể được thực hiện một cách dễ dàng hơn thông qua việc ghi nhãn hồ sơ một cách thích hợp (ví dụ, đóng dấu “bảo mật” hoặc “bí mật”), hoặc sử dụng các tệp hồ sơ có màu sắc đặc biệt (ví dụ, màu đỏ hoặc màu da cam), và bằng cách giữ những hồ sơ đã được đánh dấu một cách riêng biệt hoặc tách biệt trong một khu vực an toàn hoặc trong một tủ hồ sơ có khóa.

Tùy thuộc vào kích thước và tính chất của bí mật kinh doanh, vị trí của các thông tin tách biệt có thể là một tủ hồ sơ có khóa, một kho an ninh có người tuần tra hoặc một cơ sở lưu trữ. Cần phải có sự kiểm soát việc tiếp cận phù hợp thông qua việc cho phép và phân công trách nhiệm phù hợp, cũng như hệ thống theo dõi đối với nhân viên có quyền tiếp cận thông tin mật.

(7) Đánh dấu tài liệu

Hiện có nhiều cách hữu ích để đánh dấu thông tin hoặc bí mật kinh doanh. Hãy xem ví dụ sau:

a. KHÔNG SAO CHÉP
b. BẢO MẬT ĐỐI VỚI BÊN THỨ BA
c. CHỈ CẤP CHO ____
d. ĐỐI TƯỢNG CỦA HỢP ĐỒNG KHÔNG PHÂN TÍCH

Các ví dụ về nhãn dùng trong phân loại thông tin gồm HẠN CHẾ, TỐI ĐA, TRUNG BÌNH VÀ TỐI THIỂU.

Nhìn chung, các nhãn phải đưa ra các chỉ dẫn ngắn gọn nhưng rõ ràng cho người sử dụng về cách thức xử lý thông tin.

(8) Quản lý văn phòng và bảo mật

a. Điện thoại di động

   Việc thảo luận các chủ đề nhạy cảm trên điện thoại di động là một thực tế nguy hiểm. Thông tin bí mật có thể bị "mất" nếu không có sự hạn chế sử dụng điện thoại di động.

b. Máy fax

Thông thường, các máy fax nằm trong một khu vực không hạn chế truy cập và thường không có sự giám sát. Vấn đề thứ hai đối với máy fax là chúng cũng sử dụng những đường điện thoại - thứ mà có thể bị rò rỉ một cách khá dễ dàng.

c. Sao chụp tài liệu

Việc một nhân viên sao chụp tài liệu bí mật, sau đó chỉ lấy bản sao và bỏ đi, để quên bản gốc trong máy và người sử dụng tiếp theo có thể nhìn thấy là việc xảy ra thông thường. Cần chú ý hơn và nhớ lấy những bản gốc bí mật hoặc hồ sơ bí mật sau khi việc sao chụp hoàn tất.

d. Hủy tài liệu

Một phương pháp tốt hơn để bảo mật các hồ sơ giấy, tất nhiên là xé nhỏ giấy tờ. Việc xé nhỏ là một cách thức quan trọng trong phần lớn các chương trình bảo mật thông tin. Với nhiều loại máy trên thị trường, các doanh nghiệp có thể thực hiện việc xé nhỏ bằng nhiều cách.

e. Điện thoại

Nhiều người gọi lấy danh nghĩa là nhà nghiên cứu, nhà phân tích công nghiệp, chuyên gia tư vấn hoặc sinh viên yêu cầu cung cấp thông tin về cơ cấu tổ chức và các nhân viên của công ty – và nhiều lần họ có được các thông tin đó.

f. Tài liệu nội bộ

Bản tin, tạp chí và các ấn phẩm nội bộ khác thường chứa các thông tin hữu ích cho những kẻ rình mò, kể cả thông báo sản phẩm mới, kết quả thử nghiệm thị trường và tên các nhân viên làm việc ở các khu vực nhạy cảm (họ là các địa chỉ liên hệ tiềm năng).

g. Thùng rác

Sẽ là không an toàn nếu vứt các tài liệu vào một thùng rác đặt gần văn phòng, vì bất cứ ai đến gần thùng rác cũng có thể sử dụng lại các hồ sơ để thu thập thông tin bí mật có tính cạnh tranh.

h. Những người thích buôn chuyện và quản lý lỏng lẻo các cuộc nói chuyện

Nhân viên đang lừa dối chính mình nếu họ nghĩ rằng các cuộc nói chuyện trong giờ ăn trưa hoặc giờ giải lao, hoặc bất cứ cuộc thảo luận nào về công việc của công ty trên tàu điện ngầm, trạm xe buýt, nhà ga xe lửa hoặc nhà hàng là hoàn toàn riêng tư. Không hề là bất thường nếu người đứng gần đó có thể nghe được những cuộc đàm thoại này một cách rõ ràng.

(9) Duy trì bảo mật máy tính

Đối với phần lớn các hệ thống máy tính, ít nhất nên áp dụng hai biện pháp an ninh là:

a. Sử dụng mật khẩu để người dùng có thể truy cập vào hệ thống;
b. Việc ghi nhật ký sử dụng tự động nhằm cho phép nhân viên an ninh hệ thống có thể lần theo bất kỳ hoạt động bất thường nào hoặc truy tìm ra người đã thực hiện chúng và chỉ ra việc thay đổi được thực hiện ở đâu và khi nào.

<Kiểm soát việc tiếp cận và dán nhãn an ninh>

Việc kiểm soát quyền tiếp cận là một cách để thực thi việc cấp phép. Có nhiều cách thức để kiểm soát quyền tiếp cận, dựa trên các chính sách khác nhau và các cơ chế bảo mật khác nhau.

a. Kiểm soát quyền tiếp cận trên cơ sở nguyên tắc dựa trên các chính sách mà có thể được thể hiện rõ ràng.

b. Kiểm soát quyền tiếp cận trên mã số nhận dạng là dựa trên chính sách áp dụng cụ thể đối với từng cá nhân hoặc tổ chức, hoặc cho một nhóm chủ thể nhất định. Sau khi mã số nhận dạng được xác thực, nếu mã số thuộc danh sách có quyền tiếp cận, thì việc tiếp cận sẽ được phép.

(10) Bảo vệ bí mật được chia sẻ trong quan hệ đối tác

a. Nhân viên công ty có thể là mối đe dọa lớn nhất đối với việc bảo mật, việc bảo mật trong liên doanh, với các chuyên gia tư vấn và thậm chí cả với khách hàng cũng là rất quan trọng.

b. Đối với nhiều công ty phần mềm, việc bộc lộ nguy hiểm nhất chính là việc bán hệ thống phần mềm vì sau đó phần mềm này dễ bị đối mặt với kỹ thuật phân tích ngược. Trong phần mềm và nhiều ngành công nghiệp công nghệ cao khác, việc chuyển giao quyền sử dụng sản phẩm của công ty bạn là một cách an toàn để tự bảo vệ chống lại sự thiệt hại.

Tham khảo thêm 2-1: Thùng đựng giấy vụn có khóa

1. Ưu điểm thùng đựng giấy vụn có khóa
   (1) Giấy tờ được bảo mật từ lúc mới sử dụng đến khi hủy bỏ.
   (2) Chứng minh một cách rõ ràng và có hệ thống với khách hàng về cơ sở hạ tầng hiện tại được trang bị hệ thống bảo vệ thông tin.
   (3) Tránh được việc hủy tài liệu ngay khi tạo ra.

2. Bất lợi của thùng đựng giấy vụn có khóa
   (1) Thêm chi phí mua thùng.
   (2) Tốn thêm nhân công thu thập giấy tờ từ thùng.
   (3) Tốn không gian đặt thùng.
   (4) Tìm và theo dõi khóa thùng; cần phải quyết định xem tất cả các thùng rác phải được khóa như nhau, hay có nhiều loại khóa và ổ khóa khác nhau.
   (5) Gây phiền hà cho nhân viên bởi việc sử dụng thùng đã khóa khó hơn việc sử dụng thùng không khóa.

Tham khảo thêm 2-2: Các quy tắc cơ bản khi sử dụng mật khẩu máy tính

1. Không bao giờ chia sẻ mật khẩu với bất cứ ai.

Thậm chí khi chia sẻ với một người rất đáng tin cậy, thì vẫn có khả năng mật khẩu rơi vào tay kẻ có mục đích thù địch.

2. Tạo một mật khẩu ít nhất sáu ký tự.

Chương trình đoán mật khẩu máy tính có thể đoán được mật khẩu có ba ký tự chỉ trong vòng mười lăm phút, trong khi một mật khẩu có sáu ký tự thường sẽ mất hai năm để “phá khóa”.

3. Không tạo những mật khẩu mà người khác có thể đoán đươc (ví dụ, họ, tên, ngày sinh nhật).

4. Thay đổi mật khẩu một cách thường xuyên (ví dụ, mỗi tháng một lần).

Việc này làm giảm khả năng người nào đó đoán ra mật khẩu.

5. Giữ một bản sao mật khẩu bằng văn bản trong văn phòng.

Nếu bạn làm điều đó, đặc biệt là gần các máy tính (điều này là rất phổ biến) mục đích của việc đặt mật khẩu đã bị thất bại.

6. Hãy giữ các số điện thoại một cách cẩn thận giống như mật khẩu.

7. Không bao giờ để máy tính lại trong khi vẫn đang đăng nhập.

Điều này giúp kẻ xâm nhập không cần đoán mật khẩu mà vẫn có thể truy cập nhanh chóng nào các dữ liệu được lưu trữ trong máy tính một cách đơn giản.

NỘI DUNG 3: Sử dụng trái phép bí mật kinh doanh

1. Định nghĩa

(1) Lấy được bí mật kinh doanh một cách không công bằng là việc tiếp nhận thông tin thông qua việc trộm cắp, lừa đảo, ép buộc, hoặc các hành vi trái pháp luật hoặc không trung thực khác.

(2) Lấy được bí mật kinh doanh mặc dù đã biết về việc thông tin có được một cách trái pháp luật, hoặc có được bí mật kinh doanh mà thực sự không biết việc có được thông tin đó là không công bằng hay do vô ý nên không biết về việc có được thông tin không công bằng trước đó và, hoặc thuộc cả hai trường hợp này, nhưng vẫn sử dụng hoặc bộc lộ một bí mật kinh doanh đã có được đó.

(3) Cho dù có được một bí mật kinh doanh một cách vô tình, nhưng vẫn sử dụng hoặc bộc lộ thông tin đó kể cả sau khi biết rằng trước đó đã có người lấy nó một cách trái pháp luật.

(4) Sử dụng hoặc bộc lộ bí mật kinh doanh bằng cách vi phạm nghĩa vụ trong hợp đồng về bảo vệ bí mật kinh doanh.

a. Tiếp nhận bí mật kinh doanh đã được công bố trong các trường hợp nêu tại mục (4) nêu trên, dù do cố ý hay vô ý không biết rằng đã vi phạm nghĩa vụ hợp đồng, và sử dụng hoặc tiết lộ bí mật kinh doanh đó.
b. Sau khi vô tình giành được một bí mật kinh doanh đã được công bố theo các trường hợp nêu tại mục (4) nêu trên, tiếp tục sử dụng hoặc bộc lộ bí mật kinh doanh ngay cả khi đã biết về việc vi phạm nghĩa vụ hợp đồng hoặc vô ý không tìm hiểu về các vi phạm nghĩa vụ hợp đồng đó.

2. Bí mật kinh doanh bị đánh cắp như thế nào

(1) Gián điệp công nghiệp

Cạnh tranh gay gắt trên thị trường nội địa và xuất khẩu cũng đã dẫn đến sự gia tăng đáng báo động về các hành vi trộm cắp của người ngoài, còn được gọi là gián điệp công nghiệp. Các hoạt động gián điệp này đang gia tăng do sự gia tăng về cạnh tranh toàn cầu, chu kỳ sản phẩm ngắn hơn, lãi suất giảm dần và sự trung thành của nhân viên cũng suy giảm.

a. Những đe dọa từ bên ngoài

Những đe dọa từ bên ngoài bao gồm doanh nghiệp thuê thực hiện hành động gián điệp với tội phạm chuyên nghiệp nhắm đến những công nghệ cụ thể, tiến hành tấn công hệ thống mạng, lấy trộm máy tính xách tay:

- Truy cập vào mã nguồn, thiết kế sản phẩm, kế hoạch tiếp thị, danh sách khách hàng;
- Tiếp cận nhân viên để thu thập thông tin về công ty, v.v..

Các doanh nghiệp đang nỗ lực bảo vệ bí mật kinh doanh của họ bằng cách áp dụng các biện pháp an ninh doanh nghiệp và các điều khoản bảo mật trong hợp đồng lao động, chuyển giao quyền sử dụng công nghệ, hợp đồng phân phối và liên doanh.

b. Trộm cắp nội bộ

Trộm cắp nội bộ được thực hiện một cách cố ý bởi các công nhân bất mãn hoặc các nhân viên. Một số người cho phép mình cung cấp thông tin cho các nhân viên tình báo của đối thủ cạnh tranh, vì tiền hoặc đôi khi chỉ vì thù oán.

<u>Ví dụ</u>

Một nhân viên bị sa thải hoặc bị mất việc làm có thể trực tiếp tới một đối thủ cạnh tranh và cung cấp thông tin để trả thù hay kiếm tiền bằng cách tiết lộ những bí mật kinh doanh của bạn: như chiến lược tiếp thị, hoặc kế hoạch sản phẩm mới – dù đã ký hợp đồng bảo mật.

Đôi khi, gián điệp của đối thủ cạnh tranh có thể nghe trộm điện thoại, hoặc thường xuyên sàng lọc tài liệu rác của công ty, đột nhập vào hệ thống máy tính. Chúng có thể là những người có vẻ vô tội như các nhà phân tích nghiên cứu, các nhà phân tích kinh doanh, các chuyên gia thông tin và các nhân viên hoặc khách hàng tiềm năng - những người có được lòng tin của nhân viên công ty để có được thông tin độc quyền bằng các ưu đãi, quà tặng hoặc tống tiền.

3. Bảo vệ bí mật kinh doanh

Nhìn chung, hầu hết các nước không có một đạo luật riêng dành cho bí mật kinh doanh.

Chủ sở hữu bí mật kinh doanh phải dựa vào các quy định có liên quan của luật pháp quốc gia về chống cạnh tranh không lành mạnh và/hoặc phán quyết của tòa án về sai lầm cá nhân hoặc dân sự và bằng các điều khoản hoặc quy định thích hợp trong hợp đồng lao động và các loại hợp đồng kinh doanh khác, phù hợp với pháp luật về hợp đồng của từng nước.

(1) Pháp luật cạnh tranh không lành mạnh/các quy tắc về sai lầm

Được áp dụng đối với đối thủ cạnh tranh – người không có quan hệ hợp đồng, thực hiện hành vi sử dụng trái phép hoặc tham gia vào hành vi trộm cắp, gián điệp, hoặc sự phản bội của nhân viên. Pháp luật về những sai lầm là luật do thẩm phán tạo ra và được áp dụng ở những nước theo hệ thống thông luật.

(2) Pháp luật hợp đồng

Được áp dụng đối với các hợp đồng giữa các Bên nhằm bảo vệ bí mật kinh doanh bằng cách sử dụng điều khoản không bộc lộ hoặc điều khoản bí mật, thông qua các điều khoản chống sử dụng kỹ thuật phân tích ngược, hoặc trong trường hợp có những mối quan hệ ngầm, như giữa luật sư và khách hàng của họ, hoặc giữa ông chủ và nhân viên, v.v..

(3) Pháp luật hình sự

Được áp dụng nếu nhân viên lấy trộm những bí mật kinh doanh của một công ty hoặc một ai đó làm gián điệp hoặc tham gia vào các hành động có thể bị coi là xâm phạm quyền riêng tư, v.v. hoặc lẩn tránh những biện pháp bảo vệ kỹ thuật của các hệ thống công nghệ thông tin/hệ thống phi công nghệ thông tin.

Tham khảo thêm 3-1: Xử lý các bí mật kinh doanh đã được ghi nhớ

Khó khăn chính ở đây là tách bạch giữa bí mật kinh doanh được bảo hộ với các kiến thức và kỹ năng không được bảo hộ mà đã được lưu trong bộ nhớ của nhân viên cũ.

Tòa án một số nước đã xử lý vấn đề này theo các cách sau:

1. chủ doanh nghiệp có thể ngăn cấm nhân viên của mình sử dụng bí mật kinh doanh lưu trong bộ nhớ của nhân viên đó, tức là "sử dụng trái phép bằng bộ nhớ".
2. chủ doanh nghiệp có thể sử dụng pháp luật về bí mật kinh doanh để ra lệnh cấm nhân viên cũ làm công việc mà chắc chắn sẽ phải sử dụng bí mật kinh doanh, tức là việc “bộc lộ không thể tránh khỏi”.

Trên thực tế, cả hai trường hợp trên đều bảo vệ chống lại việc sử dụng bí mật kinh doanh đã được ghi nhớ trong não, nhưng chúng khác nhau về các hình thức áp dụng lệnh khẩn cấp tạm thời. Học thuyết về “bộc lộ không thể tránh khỏi” nên được giới hạn ở tình huống thực tế trong phạm vi hẹp, nếu nhân viên cũ không thể tránh khỏi việc sử dụng bí mật kinh doanh cụ thể để thực hiện nhiệm vụ cụ thể trong công việc mới của người đó.

NỘI DUNG 4: Xâm phạm bí mật kinh doanh

1. Cách thức xác định hành vi xâm phạm bí mật kinh doanh

Các câu hỏi chính là:

(1) Thông tin đó có thực sự là thông tin bí mật hay không?

(2) Các biện pháp hợp lý đã được áp dụng để bảo mật hay không?

Để xác định hành vi xâm phạm quyền đối với bí mật kinh doanh, chủ sở hữu bí mật kinh doanh phải chỉ ra được những điều sau:

(1) Hành vi xâm phạm được thực hiện bởi hoặc lợi thế cạnh tranh thu được của người/công ty đã sử dụng trái phép bí mật kinh doanh.

(2) Chủ sở hữu đã thực hiện các biện pháp hợp lý để bảo mật thông tin đó.

(3) Có hành vi sử dụng trái phép vì thông tin thu được đã đang được sử dụng hoặc bộc lộ theo cách vi phạm các tập quán thương mại trung thực.

2. Các biện pháp

(1) Lệnh của tòa án cấm người đó trục lợi thêm từ hoặc sử dụng trái phép bí mật kinh doanh.

(2) Lệnh của tòa án yêu cầu bồi thường bằng tiền cho những thiệt hại, dựa trên các tổn thất thực tế được gây ra do việc sử dụng trái phép bí mật kinh doanh. (Ví dụ, làm mất lợi nhuận hoặc làm giàu bất chính).

(3) Lệnh tạm giữ của tòa án, dựa trên một vụ kiện dân sự mà có thể kèm theo việc điều tra cơ sở sản xuất của bên bị kiện nhằm thu thập bằng chứng để chứng minh hành vi sử dụng trái phép bí mật kinh doanh tại phiên tòa.

(4) Sự tịch thu có cảnh báo trước các hàng hóa chứa bí mật kinh doanh bị sử dụng trái phép, hay các sản phẩm có được từ việc sử dụng hay lạm dụng nó.

(5) Tòa án có thể ra lệnh tiêu hủy các sản phẩm được sản xuất bởi hành vi xâm phạm, và/hoặc phá hủy các thiết bị dùng để thực hiện các hành vi xâm phạm này.

(6) Một số nước cho phép áp dụng các biện pháp trừng phạt đối với hành vi cố ý tiếp tay cho việc trộm cắp bí mật kinh doanh.

NỘI DUNG 5: Kiểm toán bí mật kinh doanh

1. Cách thức tiến hành kiểm toán bí mật kinh doanh

Các bước cơ bản tiến hành kiểm toán bí mật kinh doanh bao gồm:

(1) Nhận biết bí mật kinh doanh quan trọng

Làm việc với các bộ phận nghiên cứu và triển khai, sản xuất, hệ thống quản lý thông tin, bán hàng và tiếp thị, và nguồn nhân lực; so sánh lợi thế của công ty bạn về quy trình sản xuất, thành phần nguyên liệu thô, quản lý thông tin, giao dịch với khách hàng, v.v. với đối thủ cạnh tranh.

(2) Xác minh tình trạng pháp lý của công ty đối với bí mật kinh doanh

Làm việc với các bộ phận pháp lý và quản lý nhân sự để xác định việc phân công nhiệm vụ của nhân viên, chuyên gia tư vấn hoặc của những người tiền nhiệm có liên quan khác đã hoàn thành hay chưa.

(3) Xác minh rằng các thủ tục bảo mật được tuân thủ

Làm việc với bộ phận an ninh, nhân sự và các phòng ban có trách nhiệm bảo vệ bí mật kinh doanh.

(4) Xác minh rằng nhân viên, chuyên gia tư vấn, đại lý bán hàng, khách hàng và những người có liên quan khác không tiết lộ bí mật kinh doanh của bên thứ ba

Làm việc với bộ phận quản lý nhân sự để xác định xem các nhân viên mới và chuyên gia tư vấn có đồng ý bằng văn bản việc không bộc lộ thông tin bí mật của các công ty cũ hay không; làm việc với các bộ phận pháp lý, mua hàng, bán hàng và tiếp thị, nghiên cứu và triển khai, quản lý thông tin và sản xuất về các hợp đồng với bên thứ ba khác.