Bản Thông tin bảo mật Tanca

Mục Lục

Giới thiệu **1**
1.Đội ngũ Bảo mật và Chức năng **2**
2.Tuân thủ và Quyền riêng tư **2**
3. Bảo mật nhân viên **2**
4.Bảo mật ứng dụng **3**
4.1 Bảo mật môi trường hoạt động 3
4.2 Bảo mật dữ liệu 3
4.3 Bảo đảm lỗ hổng bảo mật 4
5. An ninh mạng **4**
5.1 Kiểm soát Truy cập Mạng 4
5.2 DDoS và phòng chống tấn công mạng 4
6. Bảo mật máy chủ **5**
7. Bảo mật ứng dụng **5**
7.1 Bảo mật quy trình phát triển 5
7.2 Bảo mật tài khoản 5
7.3 Lỗ hổng và ứng phó khẩn cấp 6
8. Bảo mật dữ liệu **6**
8.1 Truyền dữ liệu 6
8.2 Lưu trữ dữ liệu 6
8.3 Truy cập dữ liệu 6
8.4 Xử lý dữ liệu 7
8.5 Phát hiện bảo mật dữ liệu 7
9. An ninh cơ sở hạ tầng **8**
10. Phục hồi sau thảm họa và Liên tục cung cấp dịch vụ **8**
10.1 Sao lưu và Phục hồi sau thảm họa 8
10.2 Cam kết liên tục cung cấp dịch vụ 8
10.3 Diễn tập khẩn cấp 9
11. Quản lý Thay đổi **9**
11.1 Quản lý mã nguồn 9
11.2 Thay đổi trong hạ tầng công nghệ 9
11.3 Thay đổi cấu hình 9

Giới thiệu

Tanca là một phần mềm quản lý nguồn nhân lực tập trung vào các doanh nghiệp nhỏ và vừa tại Việt Nam và các quốc gia khác. Trọng tâm của chúng tôi là giải quyết các vấn đề sâu sắc liên quan đến lịch làm việc, theo dõi chấm công và tính lương. Giải pháp của chúng tôi có thể tích hợp với hầu hết các máy chấm công và camera trí tuệ nhân tạo tại Việt Nam.
Đối tượng khách hàng mục tiêu của chúng tôi tập trung vào các chuỗi bán lẻ, chuỗi F&B, nhà phân phối hoặc nhà sản xuất... Chúng tôi xử lý các vấn đề phức tạp về lịch làm việc và theo dõi chấm công và dẫn đầu ở Việt Nam trong lĩnh vực này. Hiện tại, chúng tôi có hơn 2500 khách hàng tại Việt Nam, và mục tiêu của chúng tôi là tiếp cận đến 30-40 nghìn doanh nghiệp. Hiện tại, có hơn 180,000 nhân viên sử dụng dịch vụ của Tanca.

1.Đội ngũ Bảo mật và Chức năng

Là một nhà cung cấp dịch vụ SaaS, Tanca đặt việc bảo mật dịch vụ và dữ liệu người dùng là ưu tiên hàng đầu. Tanca có một hệ thống cơ sở hạ tầng bảo mật hoàn chỉnh và một hệ thống bảo vệ dữ liệu và dịch vụ người dùng. Đội ngũ bảo mật của Tanca bao gồm đội quản lý bảo mật và tuân thủ, bảo mật kinh doanh, bảo mật dữ liệu, phản ứng khẩn cấp, và phát triển công cụ bảo mật. Các trách nhiệm của đội ngũ này bao gồm đánh giá bảo mật thiết kế sản phẩm, đánh giá mã nguồn, quét lỗ hổng, kiểm tra xâm nhập, thông tin về mối đe dọa, phát hiện xâm nhập, phản ứng khẩn cấp, bảo mật dữ liệu, tuân thủ bảo mật, và nhiều hoạt động bảo mật khác.

2.Tuân thủ và Quyền riêng tư

Tanca đặt mức độ ưu tiên cao về tuân thủ sản phẩm, do đó chúng tôi luôn quản lý và đảm bảo sản phẩm tuân thủ các tiêu chuẩn cao nhất trong và ngoài nước. Tanca có một đội ngũ riêng chuyên về quyền riêng tư, đánh giá các giao thức quyền riêng tư của người dùng, thiết kế bảo vệ quyền riêng tư của phần mềm, thu thập và sử dụng dữ liệu người dùng để đảm bảo dữ liệu của người dùng được sử dụng chính xác và được xử lý một cách minh bạch, hợp lý.
Tanca tích cực theo dõi và đáp ứng các tiêu chuẩn quốc tế về việc tuân thủ sản phẩm và hợp tác với các cấp cơ quan quản lý khác nhau để đảm bảo rằng các sản phẩm và dịch vụ của mình đáp ứng các yêu cầu.
Tanca đã đạt được chứng nhận ISO 27001, đây là một bộ tiêu chuẩn hệ thống quản lý bảo mật được công nhận rộng rãi. Nó được coi là một trong những tiêu chuẩn chứng nhận hệ thống bảo mật thông tin có uy tín và nghiêm ngặt nhất trên thế giới.

3. Quy trình xác thực Nhân sự

Tanca đã thiết lập quy trình bảo mật quản lý nhân sự như sau:

- Việc tuyển dụng nhân viên mới phải được phê duyệt bởi nhân viên trong lĩnh vực Nhân sự (HR) và lãnh đạo của phòng ban yêu cầu nguồn nhân lực. Quá trình tuyển dụng và kết quả được ghi lại trong hệ thống quản lý nhân sự;
- Trước khi nhân viên mới được tuyển dụng, Phòng Nhân sự phải tiến hành kiểm tra lý lịch theo quy định của pháp luật và quy định của nhà nước, tuỳ theo mức độ quan trọng của vị trí công việc, đảm bảo việc tuyển dụng tuân thủ các quy định và quy tắc của Tanca;
- Nhân viên mới được yêu cầu ký hợp đồng lao động và thoả thuận bảo mật, trong đó mô tả các nghĩa vụ và trách nhiệm của nhân viên đối với việc bảo mật thông tin;
- Bộ phận Pháp lý xem lại các điều khoản pháp lý trong thoả thuận bảo mật của nhân viên và thoả thuận bảo mật với bên thứ ba ít nhất mỗi năm một lần và cập nhật khi cần thiết, và công bố thoả thuận đã cập nhật thông qua nền tảng nội bộ để đảm bảo tất cả nhân viên và nhân viên liên quan có quyền truy cập vào các thoả thuận bảo mật mới nhất;
- Việc từ chức của nhân viên yêu cầu phải được khởi tạo bởi chính nhân viên hoặc người đứng đầu phòng ban trong hệ thống quản lý nhân sự, và phải được phê duyệt bởi Phòng Nhân sự, Phòng Công nghệ thông tin và các phòng ban chức năng khác trước khi chính thức từ chức;

Tanca đã thiết lập một hệ thống đào tạo toàn diện. Các nhân viên mới được tuyển dụng yêu cầu tham gia các khóa đào tạo về văn hóa doanh nghiệp, quy tắc và quy định, bảo mật thông tin, cơ chế khen thưởng và kỷ luật. Đồng thời, Tanca tổ chức các khóa đào tạo sau đây nhằm nâng cao kiến thức và kỹ năng chuyên môn của nhân viên, cũng như nhận thức về bảo mật thông tin theo nhiều phương thức khác nhau:

- Các khóa đào tạo liên quan đến bảo mật thông tin, nhằm nâng cao kỹ năng bảo mật thông tin của nhân viên;
- Các hoạt động liên quan đến bảo mật thông tin, nhằm tăng cường nhận thức về bảo mật thông tin;
- Chuẩn bị tài liệu về các chủ đề liên quan đến nhận thức về bảo mật thông tin và gửi đến nhân viên qua email và các áp phích.

4.Bảo mật ứng dụng

4.1 Bảo mật môi trường hoạt động

Phần mềm Tanca sẽ kiểm tra nghiêm ngặt môi trường đang hoạt động, bao gồm phát hiện root, phát hiện jailbreak, v.v. Mục đích của việc sàng lọc là đảm bảo rằng khách hàng sử dụng ứng dụng trong một môi trường an toàn và đáng tin cậy, để tránh bị hack hoặc nhiễm malware.

4.2 Bảo mật dữ liệu

Phần mềm Tanca sử dụng cơ chế bảo mật của hệ điều hành để cô lập quyền hạn giữa các ứng dụng. Toàn bộ tương tác giữa khách hàng và máy chủ được mã hóa bằng HTTPS hoặc WSS.

4.3 Bảo đảm lỗ hổng bảo mật

Tanca có một đội ngũ khai thác lỗ hổng bảo mật di động chuyên nghiệp để tiến hành đánh giá bảo mật và khai thác lỗ hổng cho hệ điều hành Android, iOS, cũng như phát hiện lỗ hổng bảo mật của các thành phần bên thứ ba của ứng dụng (thư viện, SDK), nhằm loại bỏ các lỗ hổng tồn tại trong ứng dụng càng nhiều càng tốt để đảm bảo an ninh của ứng dụng.

5. An ninh mạng

5.1 Kiểm soát Truy cập Mạng

Tanca sử dụng Amazon Web Services (AWS) để cung cấp các dịch vụ hạ tầng, bao gồm phòng máy chủ, mạng, máy chủ, hệ điều hành, v.v., và cung cấp dịch vụ bảo mật hạ tầng. Nhờ bởi AWS, Tanca nâng cao kiểm soát bảo mật trong việc truy cập máy chủ, và tất cả các dịch vụ phải được hoạt động và được kiểm tra qua máy Bastion.
Tất cả nhân viên cần được xác thực để truy cập vào tài nguyên nội bộ. Sau khi xác nhận danh tính, nhân viên chỉ có phân quyền theo mặc định. Việc cấp quyền mới cần được phê duyệt và ghi nhận bởi các nhân viên có liên quan và có trách nhiệm. Quyền hạn có ngày hết hạn, và hệ thống sẽ tự động thu hồi quyền hạn sau ngày hết hạn. Các hoạt động dịch vụ trực tuyến của nhân viên được thực hiện thông qua máy bastion, và tất cả các nhật ký hoạt động được lưu giữ cho mục đích kiểm tra sau này.
Tất cả nhân viên ngoài giới hạn mạng nội bộ của công ty cần phải truy cập vào tài nguyên nội bộ của Tanca thông qua kết nối VPN. Phòng nội bộ kiểm toán và kiểm soát của Tanca sẽ

kiểm tra nhật ký truy cập, tìm kiếm các bản ghi vi phạm quy định, và xử lý các khiển trách tương ứng.

5.2 DDoS và phòng chống tấn công mạng

Dịch vụ Tanca cung cấp cho khách hàng trên toàn thế giới quyền truy cập vào mạng của mình thông qua CDN (Mạng phân phối nội dung) và tăng tốc độ động, cũng như quyền truy cập vào dịch vụ phía sau thông qua cân bằng tải của AWS. Khi gặp phải cuộc tấn công DDoS, phòng vệ sẽ được thực hiện thông qua dịch vụ làm sạch mạng của Cloudflare chẳng hạn

5.3 Mã hóa truyền dẫn mạng

Dịch vụ Tanca được truyền qua giao thức HTTPS và WSS trên cả mạng nội bộ và mạng ngoài, đảm bảo tính bảo mật của quá trình truyền dẫn và ngăn chặn việc nghe trộm và phá hoại.

6. Bảo mật máy chủ

Tanca sử dụng các máy chủ đám mây của AWS để phục vụ khách hàng của mình. Amazon cung cấp bảo mật cho các máy chủ đám mây từ lớp vật lý đến lớp ảo hóa. Để biết chi tiết về bảo mật máy chủ đám mây do AWS cung cấp, vui lòng xem Báo cáo về Bảo mật Đám mây của Amazon tại đây:
https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

7. Bảo mật ứng dụng

7.1 Bảo mật quy trình phát triển

Chúng tôi nỗ lực kiểm soát các rủi ro bảo mật từ nguồn gốc của các lỗ hổng bảo mật. Tất cả các nhà phát triển và quản lý sản phẩm sẽ nhận được đào tạo về bảo mật để hiểu về

nguyên nhân của các lỗ hổng bảo mật và củng cố kiến thức lập trình. Đội ngũ bảo mật sẽ đánh giá các thư viện và công cụ của bên thứ ba được sử dụng trong sản phẩm và khai thác các lỗ hổng có thể để đảm bảo không có lỗ hổng nào xảy ra, sau đó họ sẽ làm việc cùng với nhóm sản phẩm để tiến hành đánh giá bảo mật của thiết kế và mã nguồn.

7.2 Bảo mật tài khoản

Truy cập của người dùng vào hệ thống Tanca được xác thực bằng cách sử dụng email/mật khẩu hoặc số điện thoại với mã xác minh ngẫu nhiên. Mỗi tài khoản chỉ có thể đăng nhập trên 1 thiết bị cùng lúc. Hệ thống kiểm soát rủi ro có các chức năng bảo vệ chống lại đăng ký độc hại, tấn công liệt kê thông tin xác thực và các chức năng bảo vệ khác.

7.3 Lỗ hổng và ứng phó khẩn cấp

Đội bảo mật của Tanca ghi nhận và xem xét các lỗ hổng được báo cáo từ bên ngoài, đánh giá mức độ nghiêm trọng và độ khẩn cấp để khắc phục. Đội bảo mật luôn hoạt động 24/7, cho phép họ nhanh chóng phản ứng với các sự cố bảo mật. Trong trường hợp xảy ra sự cố bảo mật, đội bảo mật sẽ phân loại sự kiện dựa trên kế hoạch bảo mật khẩn cấp và khởi động quy trình ứng phó khẩn cấp để ngăn chặn sự cố bảo mật không lan rộng thêm. Phương pháp tiếp cận tích cực này giúp giảm thiểu rủi ro bảo mật.

8. Bảo mật dữ liệu

Tanca có một quy trình quản lý vòng đời dữ liệu hoàn chỉnh với đảm bảo kỹ thuật cho mỗi giai đoạn của vòng đời dữ liệu, bao gồm quá trình hình thành, lưu trữ, sử dụng, truyền tải, chia sẻ và hủy bỏ.

8.1 Truyền dữ liệu

Tanca cung cấp cho người dùng các kênh truyền dữ liệu hỗ trợ các giao thức mã hóa an toàn. Các quá trình truyền dữ liệu như lấy tin nhắn, xác thực định danh, hướng dẫn hoạt động được mã hóa thông qua giao thức HTTPS và một khóa RSA 2048-bit. Đẩy tin nhắn sử dụng giao thức WSS để bảo vệ dữ liệu được truyền thông qua mã hóa.

8.2 Lưu trữ dữ liệu

Tanca sử dụng cơ chế khóa để hỗ trợ việc lưu trữ dữ liệu được mã hóa. Tanca đã phát triển một phương pháp phân loại và quản lý dữ liệu toàn diện, và đã phân loại và phân loại nghiêm ngặt thông tin người dùng được thu thập bởi Tanca. Tanca đã mã hóa dữ liệu nhạy cảm được lưu trữ trong hệ thống, đồng thời bảo vệ hiệu quả thông tin người dùng.

8.3 Truy cập dữ liệu

Quyền truy cập vào dữ liệu người dùng của Tanca được giới hạn một cách nghiêm ngặt thông qua các quyền hạn. Người dùng không thể truy cập vào các tài khoản của nhau mà không có sự cho phép.
Việc nhân viên của Tanca truy cập vào dữ liệu người dùng được giới hạn một cách nghiêm ngặt và được kiểm tra, và nhân viên không có quyền truy cập vào bất kỳ dữ liệu người dùng nào mặc định. Yêu cầu truy cập đặc biệt phải được sự cho phép rõ ràng của người dùng và một quy trình phê duyệt nội bộ nghiêm ngặt để có được quyền truy cập tạm thời, trong đó các quyền hạn được thu hồi ngay sau khi hoàn thành. Lịch sử đăng nhập, hoạt động, và thay đổi quyền truy cập vào tất cả các máy chủ trong môi trường trực tuyến của Tanca được ghi lại.
Tanca sẽ không tiết lộ thông tin người dùng công khai trừ khi có sự đồng ý của người dùng. Tuy nhiên, trong trường hợp dữ liệu của người dùng được yêu cầu theo quy định của pháp luật, yêu cầu bắt buộc từ các cơ quan hành chính hoặc yêu cầu của tòa án, Tanca có thể tiết lộ thông tin cá nhân của người dùng cho cơ quan quản lý thực thi pháp luật hoặc cơ quan chức năng theo yêu cầu về loại dữ liệu cá nhân cần yêu cầu. Khi chúng tôi nhận được yêu cầu tiết lộ, chúng tôi sẽ tuân thủ theo quy định của luật pháp và cấp các tài liệu pháp lý tương ứng. Chúng tôi chỉ cung cấp dữ liệu mà các cơ quan thực thi pháp luật có quyền hợp pháp để thu thập cho mục đích điều tra cụ thể. Các tài liệu chúng tôi tiết lộ đều được bảo vệ bằng các biện pháp mã hóa, tuân thủ theo luật pháp và quy định.

8.4 Xử lý dữ liệu

Khi chấm dứt dịch vụ đối với một người dùng, quản trị viên của Tanca sẽ xóa thông tin tài khoản người dùng và xóa vĩnh viễn dữ liệu của người dùng theo quy định của luật pháp địa phương.
Các quản lý có thể tái kích hoạt tài khoản của nhân viên. Khi một quản lý xóa một nhân viên, Tanca sẽ giấu danh tính và dữ liệu của tài khoản yêu cầu dựa trên đơn đăng ký của quản trị viên đơn vị sử dụng.
Khi Tanca ký hợp đồng dịch vụ với tổ chức người dùng, quy định rằng khi dịch vụ bị chấm dứt, dữ liệu tương ứng sẽ được xử lý theo yêu cầu của tổ chức người dùng.
Ngoài người dùng từ các đơn vị, Tanca cũng cung cấp dịch vụ cho người dùng cá nhân. Khi một người dùng cá nhân cần xoá tài khoản, họ cần liên hệ với Tanca, đồng thời Tanca sẽ

cung cấp gói cài đặt Tanca với chức năng xoá tài khoản thông qua chức năng dịch vụ khách hàng của Tanca. Sau khi cài đặt, người dùng có thể yêu cầu xoá tài khoản trên hệ thống và Tanca sẽ giấu danh tính và dữ liệu của tài khoản yêu cầu trong cơ sở dữ liệu của Tanca.

8.5 Phát hiện bảo mật dữ liệu

Hành vi đăng nhập, và các hoạt động khác trong môi trường trực tuyến Tanca đều được ghi lại.

9. An ninh cơ sở hạ tầng

Tanca sử dụng dịch vụ của Amazon Web Services (AWS) để phục vụ khách hàng ở các khu vực khác nhau trên thế giới. Là một trong những nhà cung cấp dịch vụ đám mây của Tanca, AWS cung cấp các dịch vụ như máy chủ đám mây. AWS tự mình vận hành, quản lý và kiểm soát tất cả các phần cứng và phần mềm của nó từ tầng vật lý đến tầng ảo hóa. Là một trong những nhà cung cấp dịch vụ đám mây hàng đầu thế giới, Amazon có khả năng bảo mật hàng đầu ngành công nghiệp để cung cấp cho người dùng độ an toàn của hạ tầng. Để biết thêm chi tiết về bảo vệ hạ tầng dịch vụ đám mây do AWS cung cấp, vui lòng tham khảo Báo cáo an ninh của AWS tại đường dẫn sau:
https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

10. Phục hồi sau thảm họa và Liên tục cung cấp dịch vụ

10.1 Sao lưu và Phục hồi sau thảm họa

Tanca đã thành lập Chính sách Quản lý Sao lưu và Phục hồi Dữ liệu để chuẩn hóa chiến lược sao lưu, thời gian lưu trữ dữ liệu sao lưu và phương pháp kiểm tra phục hồi, v.v. Các cơ sở dữ liệu kinh doanh được chụp ảnh và sao lưu định kỳ.

10.2 Cam kết liên tục cung cấp dịch vụ

Hệ thống truy cập vào lớp dịch vụ được triển khai với tính sẵn sàng cao và thông qua dịch vụ cổng vào công cộng. Phía sau sử dụng kiến thức đa mẫu để đảm bảo tính tin cậy của

dịch vụ. Thông qua giám sát chi tiết, nếu xảy ra tắc nghẽn hoặc lỗi, chế độ hoạt động bị giảm sẽ được sử dụng để đảm bảo tính sẵn sàng của dịch vụ.
Tanca đã phát triển kế hoạch cung cấp hướng dẫn về phản ứng khẩn cấp và biện pháp phục hồi cho các tình huống có thể dẫn đến gián đoạn kinh doanh. Tanca thực hiện phân tích tác động đến hoạt động kinh doanh và đánh giá nguy cơ mỗi năm một lần để xác định các quy trình kinh doanh quan trọng và các mối đe dọa có thể gây gián đoạn cho hoạt động kinh doanh và tài nguyên của Tanca; định nghĩa các chỉ số như thời gian gián đoạn tối đa có thể chấp nhận được, mục tiêu thời gian phục hồi, và mức độ dịch vụ tối thiểu, v.v.; phát triển các chiến lược phản ứng tương ứng cho các tình huống gián đoạn khác nhau của các dòng kinh doanh khác nhau của Tanca.

10.3 Diễn tập khẩn cấp

Tanca có cơ chế diễn tập khẩn cấp hoàn chỉnh và thường xuyên tiến hành các cuộc diễn tập lỗi với sự tham gia của các đội như đội phát triển, đội bảo mật, đội vận hành và bảo trì, v.v.

11. Quản lý Thay đổi

11.1 Quản lý mã nguồn

Tanca đã phát triển một quy trình quản lý mã nguồn nghiêm ngặt, và các nhà phát triển chỉ có thể truy cập và quản lý kho mã nguồn tương ứng với nhóm của họ. Các nhân viên Nghiên cứu và Phát triển (R&D) chỉ có quyền truy cập vào kho mã nguồn thuộc về nhóm của họ. Chủ sở hữu của kho mã nguồn cụ thể cần được đặt cho mỗi dự án. Nếu nhân viên R&D yêu cầu truy cập vào kho mã nguồn thuộc về nhóm khác, đơn xin được nộp trong kho mã nguồn. Kho mã nguồn sẽ tự động cấp quyền truy cập cho người nộp đơn sau khi nhận được sự chấp thuận từ người đứng đầu nhóm của người nộp đơn và chủ sở hữu của kho mã nguồn được đăng ký.

11.2 Thay đổi trong hạ tầng công nghệ

Tanca quản lý việc truy cập mạng bằng cách triển khai Danh sách Kiểm soát Truy cập (Access Control List - ACL) trên ranh giới mạng công cộng. Nếu có yêu cầu thay đổi cấu hình ACL cơ bản và chính sách kiểm soát truy cập mạng, nhân viên vận hành đăng ký qua nền tảng quy trình hệ thống. Một kỹ sư từ Bộ phận Hệ thống sẽ thực hiện thay đổi sau khi

đánh giá tính hợp lý của yêu cầu thay đổi. Chỉ có các kỹ sư được ủy quyền từ Bộ phận Hệ thống mới được cấp quyền truy cập để thay đổi cấu hình kiểm soát truy cập mạng.

11.3 Thay đổi cấu hình

Tanca thực hiện kiểm toán nội bộ (internal audit) hàng năm bởi đội ngũ nội bộ của mình để đánh giá hiệu quả hoạt động của hệ thống kiểm soát nội bộ của Tanca, bao gồm cả các kiểm soát liên quan đến quản lý thay đổi (change management). Kết quả kiểm toán được tóm tắt trong báo cáo kiểm toán nội bộ. Nếu phát hiện bất kỳ ngoại lệ nào, Bộ Phận Kiểm Toán Nội Bộ và Kiểm Soát Nội Bộ sẽ thông báo cho đội người phụ trách để thực hiện các biện pháp khắc phục và theo dõi tình trạng khắc phục.