۳. مرامنامه ترک تیم برای مهندسان تیم DevOps

مرامنامه که معتقدم به‌کارگیری آن می‌تواند به‌عنوان یک راهنما برای انتقال دانش و تضمین روابط کاری مثبت در آینده مفید باشد.

علاوه بر مواردی که در مرامنامه عمومی تیم قبلی ارائه شد، به عنوان یک مهندس DevOps، قبل از ترک تیم، باید از مراحل زیر عبور کنید:

انتقال دانش: تمامی دانش و تجربه‌ای که در طول حضور در تیم به دست آورده‌اید را به تیم انتقال دهید. این شامل اطلاعات مربوط به سیستم‌ها، فرآیندها، تکنولوژی‌های مورد استفاده، اسکریپت‌ها و ابزارهای اتوماسیون است. همچنین به تیم کمک کنید تا دانش شما در هر زمینه‌ای که ممکن است مورد احتیاج قرار بگیرد را به دست آورد.

حفظ محرمانگی: تمامی اطلاعات حساسی که در طول حضورتان در تیم دسترسی داشته‌اید را محرمانه نگه دارید و هیچ‌گونه اطلاعاتی را به شخصی‌های خارج از شرکت ارائه ندهید.

حذف دسترسی‌ها و حساب‌ها: قبل از ترک تیم، اطمینان حاصل کنید که تمامی دسترسی‌هایی که به سیستم‌ها، سرویس‌ها و ابزارهایی که در آنها کار کرده‌اید دسترسی دارید را لغو کنید. همچنین اطمینان حاصل کنید که حساب‌های کاربری شما در سیستم‌های داخلی و خارجی شرکت غیرفعال شده‌اند.
(به لیست شماره یک ضمیمه این مرامنامه مراجعه شود)

ارزیابی و تجزیه و تحلیل: اگر امکان دارد، به تیم کمک کنید تا عملکرد و نقاط ضعف سیستم‌هایی که به آنها دسترسی داشته‌اید را بررسی کنند و راهکارهایی را پیشنهاد دهید که می‌توانند عملکرد سیستم‌ها را بهبود بخشند.

تشکر: در نهایت، از تیم برای فرصتی که برای کار در این تیم داشتید تشکر کنید. به تیم بگویید که چه چیزهایی در این تیم یاد گرفتید و چگونه این تجربه شما را در آینده بهتر خواهد کرد.

من متعهد به احترام در به کارگیری این مرامنامه هستم و با تیم در این راستا به‌منظور تضمین یک انتقال موثر همکاری خواهم کرد. از فرصتی که برای کار در این تیم داشتم، قدردانی می‌کنم و برای تیم و شرکت در آینده بهترین‌ها را آرزو می‌کنم.

با احترام.

(پیش نویس نسخه یک مرامنامه ارسلان سفیدگر ۱۴۰۲/۰۲/۱۸)

ضمیمه ها

لیست شماره یک:

حساب‌های ایمیل: تمامی حساب‌های ایمیلی که با آنها در طول حضور در تیم کار کرده‌اید (مانند حساب‌های Gmail، Outlook و...) را غیرفعال کنید. این اقدام به جلوگیری از دسترسی به پست‌های الکترونیکی شما و اطلاعات حساس مرتبط با شرکت کمک خواهد کرد.
حساب‌های سرویس دهندگان ابری: اگر شرکت شما از سرویس‌های ابری مانند AWS، Azure و Hetzner استفاده می‌کند، اطمینان حاصل کنید که حساب‌های خود در این سرویس‌ها را غیرفعال کرده‌اید. این اقدام به جلوگیری از دسترسی به سیستم‌ها و داده‌های حساس مرتبط با شرکت کمک خواهد کرد.
حساب‌های نرم افزارهای شرکت: اگر شما از نرم افزارهایی مانند Slack، Trello و Jira استفاده می‌کند، اطمینان حاصل کنید که حساب‌های شما در این نرم افزارها را غیرفعال کرده‌اید. این اقدام به جلوگیری از دسترسی به اطلاعات حساس مرتبط با شرکت کمک خواهد کرد.
حساب‌های شبکه‌های اجتماعی: اگر شرکت شما از شبکه‌های اجتماعی مانند LinkedIn و Twitter برای ارتباط با مشتریان و همکاران استفاده می‌کند، اطمینان حاصل کنید که حساب‌های خود در این شبکه‌ها را غیرفعال کرده‌اید. این اقدام به جلوگیری از دسترسی به اطلاعات حساس مرتبط با شرکت کمک خواهد کرد.
دسترسی‌های داخلی: اطمینان حاصل کنید که تمامی دسترسی‌هایی که به سیستم‌ها و داده‌های شرکت داشتید را لغو کرده‌اید. این اقدام به جلوگیری از دسترسی به داده‌های حساس و بهبود امنیت شرکت کمک خواهد کرد.
ابزارهای اتوماسیون: اگر شما از ابزارهای اتوماسیونی مانند Puppet، Ansible و Chef برای مدیریت سیستم‌های شرکت استفاده می‌کردید، اطمینان حاصل کنید که دسترسی‌های خود به این ابزارها را لغو کرده‌اید. این اقدام به جلوگیری از دسترسی به سیستم‌های شرکت و بهبود امنیت شرکت کمک خواهد کرد.