جمهوری اسلامی ایران
قوه قضائیه
سازمان بازرسی کل کشور

گزارش پژوهشی

سال هفدهم، شماره ۱۵۶، شهریور ۱۴۰۳

سیستم های افشاگری درون سازمانی

بهترین اصول اجرایی برای سازمان های دولتی و خصوصی

نویسنده: ماری تراکول
مترجم: دکترغلامحسین همایونی

ویراستار و صفحه‌آرا: محمد روشنی

انتشارات سازمان بازرسی کل کشور

مرکز آموزش و پژوهش های سلامت اداری و مبارزه با فساد

تهران: خیابان آیت‌الله طالقانی، تقاطع شهید سپهبد قرنی، سازمان بازرسی کل کشور
شماره تماس: ۸۸۸۴۴۶۱۴ -۰۲۱ ● Bazrasi.nashr@136.ir

فهرست

گزارش در یک نگاه

اصطلاح اعلان جرم (افشاگری و یا سوت‌زنی)، عموماً به فرایند گزارش و افشای یک اتفاق یا رویه خلاف قانون در یک ساختار، از سوی یک شخص افشاگر در همان ساختار یا خارج از آن، اطلاق می‌شود. اعلان‌کننده، معمولاً یکی از کارمندان سازمان دولتی یا خصوصی است که رفتار خلاف قانون کارفرمایان خود را گزارش می‌دهد. این فرد، می‌تواند کارمند فعلی یا سابق نهاد موردنظر باشد. این در حالی است که قانون‌شکنی می‌تواند درگذشته به‌وقوع پیوسته باشد، هم‌اکنون در جریان باشد یا در آینده بیم وقوع آن برود.

افشاگری یکی از ابزارهای مهم در مبارزه با فساد و تقویت شفافیت و عدالت در جوامع است. علاوه‌براین در کنوانسیون‌ها و اسناد مهم بین‌المللی برای مبارزه با فساد و ارتقاء صداقت و درستکاری به کشورهای جهان در راستای قانون‌گذاری برای حمایت از افشاگران فساد توصیه‌های لازم صورت پذیرفته است.

در همین راستا «قانون حمایت از گزارشگران فساد» در تاریخ ۱۴۰۲/۸/۱۴ توسط مجلس شورای اسلامی تصویب و جهت اجرا به دولت ابلاغ گردید.

گزارش حاضر ترجمه‌ای است از «**سیستم‌های افشاگری درون‌سازمانی**» تهیه‌شده توسط سازمان شفافیت بین‌الملل[1] (TI) که مشتمل بر توصیه‌ها و راهکارهایی برای راه‌اندازی این سیستم در درون سازمان‌های خصوصی و دولتی می‌باشد. در این گزارش به موضوعاتی ازقبیل اهداف یک سیستم افشاگری درون‌سازمانی، مزایای آن، مبانی و موارد اساسی در راه‌اندازی سیستم‌های افشاگری درون‌سازمانی (چشم‌انداز، نقش‌ها و مسئولیت‌ها، اطلاعات و ارتباطات، سازوکارها)، پشتیبانی و حفاظت از افشاگران و

1. Transparency International

حفاظت از سایر افراد دخیل در افشاگری و نحوه رصد و ارزیابی پیوسته سیستم افشاگری درون‌سازمانی اشاره گردیده است.

علاوه‌براین، نحوه ایجاد سیستم اطلاعات و ارتباطات درون‌سازمانی، گسترش فرهنگ سازمانی در زمینه اعتماد، شفافیت و پاسخ‌گویی، مدیریت اخلاقی و نحوه تشویق و قدردانی از افشاگران، بسترهای نرم‌افزاری[1] گزارش‌دهی آنلاین، مقررات عمومی ثبت، نگهداری و حفاظت از داده‌ها و نحوه پیشگیری از رفتارهای آسیب‌زا به افشاگران مورد کنکاش و بررسی قرار گرفته و توصیه‌های ارزشمندی به سازمان‌ها و نهادهای دولتی و خصوصی ارائه شده است.

امید است گزارش حاضر بتواند در ایجاد دیدگاهی همه‌جانبه به مدیران خصوصاً در «***دفاتر مدیریت عملکرد***» سازمان‌های دولتی و خصوصی برای جلوگیری از انحرافات سازمانی به‌وسیله راه‌اندازی سیستم افشاگری درون‌سازمانی، مؤثر و کارساز واقع گردد.

مرکز آموزش و پژوهش‌های سلامت اداری و مبارزه با فساد

1. Platform

مقدمه

افشاگری یکی از کارآمدترین شیوه‌های برملا ساختن فساد، کلاهبرداری، سوءمدیریت و دیگر تخلفاتی است که سلامت و امنیت همگانی، سلامت مالی و حقوقی بشر و محیط زیست را تهدید می‌کنند.

افشاگری به‌منزله آشکار کردن اطلاعات مرتبط با اشخاص و شرکت‌های تجاری است که مظنون به ارتکاب تخلف می‌باشند. در بیشتر موارد سازمان‌ها در ساختار خود می‌توانند به خطای صورت‌گرفته رسیدگی نمایند و در عمل بیشتر افشاگران گزارش‌های خود مبنی بر گمان تخلف را در چارچوب ساختار سازمان خود ارائه می‌دهند؛ ازاین‌رو بسیار مهم است که سازمان‌ها چه در بخش دولتی و چه در بخش خصوصی، سازوکارهای امن و کارآمدی را برای دریافت و رسیدگی به گزارش‌های افشاگری فراهم سازند و تمام قد از افشاگران خود حراست نمایند.

به‌همین‌خاطر است که شمار فزاینده‌ای از قوانین در کشورهای گوناگون، سازمان‌ها را ملزم به راه‌اندازی «سیستم‌های افشاگری درونی»[1] (IWS) نموده‌اند. این سازوکارها گاه به‌نام «سیستم اعلام» یا «سیستم گزارش‌دهی درونی» خوانده می‌شوند. این قوانین در کشورهای اروپایی از دسامبر ۲۰۲۱ به‌صورت یکپارچه درآمده و در چارچوب «بخشنامه حفاظت از افشاگر»[2] اتحادیه اروپا به‌کار گرفته می‌شود.

بااین‌وجود سازمان‌ها نباید سیستم افشاگری درونی را به چشم یک اجبار قانونی ببینند. اجرای کارآمد این سیستم‌ها به سازمان‌ها کمک می‌کند از پیامدهای سوءرفتار در امان باشند و مواردی همچون مسئولیت حقوقی، آسیب ماندگار به اعتبار و زیان‌های سنگین مالی گریبانگیر آن‌ها نشود. سیستم‌های افشاگری درونی (IWS) شرایط لازم را

1. Internal Whistle Blowing Systems (IWS)
2. Whistleblower Protection Directive

فراهم ساخته تا پرسنل و دیگر طرف‌های مرتبط بتوانند هرگونه کنش غیراخلاقی یا غیرقانونی را اعلام کنند. به‌این‌ترتیب سیستم افشاگری درونی بستری برای فرهنگ سازمانی مبتنی بر اعتماد، شفافیت و پاسخ‌گویی ایجاد می‌کند. ازاین‌روست که سازمان‌ها در زمینه‌هایی مانند فرهنگ، برند، ارزش‌آفرینی و رشد از IWS سود می‌برند.[1]

هدف از نگارش این پژوهش، پشتیبانی از اجرای کارآمد سیستم‌های افشاگری درونی می‌باشد. همچنین امید می‌رود مطالب ارائه‌شده در اینجا، به سازمان‌هایی که در چارچوب اتحادیه اروپا فعالیت می‌کنند کمک کند تا تعهدات خود را بر مبنای بخشنامه حفاظت از افشاگری اتحادیه اروپا به انجام برسانند.

در ادامه به‌منظور اجرای هرچه بهتر IWS [2] بر اساس بخشنامه حفاظت از افشاگر اتحادیه اروپا و رهنمودهای ISO در زمینه سیستم‌های مدیریت افشاگری اصولی ارائه می‌گردد که برای موارد زیر سودمند می‌باشند:

- اجرای کارآمد سیستم‌های افشاگری درونی در سازمان‌ها در تمامی حوزه‌ها (دولتی، خصوصی و حوزه سوم[3])، حیطه‌های قانونی مانند سازمان‌های

---

۱. برای نمونه مراجعه شود به: «شواهد به‌کارگیری و اثربخشی سیستم‌های افشاگری درونی» (۲۰۲۰) از اشتفن اشتوبن و کایل ولش (Stephen Stubben and Kyle Welch)؛ «پیروی به‌واسطه فرهنگ و ارزش‌های شرکت: پژوهشی بین‌المللی برمبنای نمونه پیشگیری از فساد» (۲۰۱۹) از باسمن، کی - دی و نیمه چک (Bussmann, K.-D., & Niemeczek)، انتشار یافته در *Journal of Business Ethics*, 157(3), 797–811. «از بی‌علمی در برابر افشاگری بیرونی: تاثیر فرهنگ اخلاقی سازمان‌ها بر واکنش کارکنان نسبت به تخلف دیده شده» (۲۰۱۱) از کاپتاین (Kaptein) برگرفته از: *Journal of Business Ethics*, 98, 513–530. «تشویق کارکنان به گزارش‌دهی درونی رفتار غیراخلاقی: همه باید دست به‌کار شوند» (۲۰۱۳) از مایر، نورمحمد، لیب تروینو، شاپیرو و اشمینک (D.M., Nurmohamed, S., Klebe Treviño, L., Shapiro, D.L., & Schminke, M.). رفتارسازمانی و فرایندهای تصمیم‌گیری انسانی، صفحات ۱۲۱ و ۱۰۳ - ۸۹. «تأثیر عدالت سازمانی بر افشاگری در حسابرسی (۲۰۱۰) از سایفرت، سوویینی، جویرمان و تورنتون (Seifert, D. L., Sweeney, J. T., Joireman, J., & Thornton, J. M)، برگرفته از: *Accounting, Organizations and Society*, 35(7), 707-717.

۲. در سرتاسر این متن، عبارت IWS به معنای «سیستم‌های افشاگری درونی» می‌باشد. (مترجم)

۳. منظور از حوزه سوم، سازمان‌های مردم‌نهاد می‌باشد. (مترجم)

بین‌المللی همچون زیرمجموعه‌های سازمان ملل متحد که در زمینه طراحی و اجرای IWS فعال می‌باشند.

- سیاست‌گذارانی که قوانین، مقررات و آیین‌نامه‌های ملی در زمینه IWS طرح می‌کنند.
- مسئولان سازمانی و دیگر دست‌اندرکاران همچون انجمن‌های بازرگانی، اتحادیه‌های صنفی به‌منظور طراحی یا صیانت از ابزارهای IWS ویژه‌ای که با توجه به مشخصات هر کشور به‌وجود می‌آیند.

هدف‌های یک سیستم افشاگری درونی

- توانمندسازی پرسنل و دیگر طرف‌های دخیل در راستای اعلام کردن تخلف.
- فراهم نمودن شرایط شناسایی خطای انجام‌شده در زمان مناسب و رسیدگی دقیق به آن در هر سازمان یا برای آن؛
- پیشگیری و رساندن آسیب وارده به سازمان به کمترین میزان ازجمله مسئولیت حقوقی، زیان‌های مالی سنگین و آسیب بلندمدت به اعتبار سازمان و کاهش اعتماد همگانی به آن. این مهم با ایجاد امکان شناسایی زود هنگام و اصلاح خطای صورت‌گرفته محقق می‌گردد؛
- پیشگیری و رساندن آسیب به منافع همگانی به کمترین میزان؛ ازجمله آسیب به سلامت همگانی، حقوق بشر و محیط‌زیست؛
- محافظت از افشاگران و اشخاص ثالثی که در خطر اقدام آسیب‌زا قرار می‌گیرند؛
- ایجاد امکان یادگیری و واکنش برای سازمان‌ها.

- پرورش یک فرهنگ سازمانی مبتنی بر اعتماد، شفافیت و پاسخ‌گویی که به پیشگیری از تخلف کمک می‌کند.

مزایای سیستم افشاگری درونی

سیستم‌های افشاگری درونی برای تمامی سازمان‌ها از هر نوع، مزایای حقیقی و بسیار ارزشمندی دارند:

۱. **نمایش تعهد سازمان نسبت به پاکدستی و مسئولیت اجتماعی**

سهامداران خواهان برنامه‌های اخلاقی داخلی کارآمدی هستند که بتواند در بلندمدت به ارزش‌آفرینی و رشد شرکت کمک کند. وجود سیستم‌های افشاگری درونی به سهامداران و همگان نشان می‌دهد که مدیریت ریسک، مسئولیت اجتماعی و پاکدستی جز اولویت‌های سازمان است.

۲. **پیشگیری و به حداقل رساندن مسئولیت**

شناسایی زودهنگام تخلف به سازمان‌ها امکان می‌دهد پیش از آنکه مشکل گسترش پیدا کرده و به سطح ایجاد مسئولیت‌های قانونی برسد، به این موارد رسیدگی نمایند. سازمان‌ها همچنین در صورت کشف زودهنگام تخلف قادر خواهند بود داوطلبانه مسئله کشف‌شده را به نهادهای نظارتی گزارش دهند؛ درصورتی‌که این گزارش‌های زودهنگام به مقامات مربوطه داده نشود، سازمان‌های قضایی و بازرسی خود اقدام کرده و ممکن است در ارزیابی‌های خود به این نتیجه برسند که سازمان مورد نظر به وظیفه قانونی خود عمل نکرده است.

۳. **پیشگیری و به حداقل رساندن زیان‌های مالی**

سیستم‌های گزارش‌دهی درونی می‌توانند از زیان‌های ناشی از کلاهبرداری و مسئولیت پاسخ‌گویی (مانند مجازات‌های مدنی و کیفری) پیشگیری کرده یا

آن‌ها را کاهش دهند. افزون‌براین، آگاهی از وجود چنین سیستم‌هایی در ساختار سازمان‌ها می‌تواند افراد را از تخلف باز داشته و ترس از گزارش شدن، آنان را برای جلوگیری از خطا ترغیب نمایند.[۱]

۴. پیشرفت پیوسته در پیروی از قانون و مدیریت ریسک

گزارش شدن اطلاعات مربوط به مسائل به‌وجودآمده با سیستم‌های گزارش‌دهی درونی به سازمان‌ها امکان می‌دهد، سیاست‌ها و سازوکارهای خود را بهبود داده و منابع تازه موردنیاز برای کاهش بروز ریسک را شناسایی نمایند.

۵. تقویت اعتبار

یک تخلف اخلاقی یا قانونی پیامدهایی دارد که می‌تواند ارزش برند یک سازمان را از بین ببرد. ازجمله این پیامدها می‌تواند به کاهش سرمایه‌گذاری، کاهش سود و پایین آمدن روحیه پرسنل اشاره کرد. با وجود سازوکارهای گزارش‌دهی درونی، رهبران سازمان می‌توانند از آسیب به اعتبار سازمان خود پیشگیری کرده یا دست‌کم آن را به حداقل برسانند.

۶. پیشرفت فرهنگ سازمان

اگر سیستم‌های گزارش‌دهی درونی از پشتیبانی رهبران سازمان و پاسخ‌گویی صنفی برخوردار باشند، قادرند فرهنگی برمبنای اعتماد، شفافیت و پاسخ‌گویی در سازمان به‌وجود آورند، به‌نحوی‌که بر عملکرد تمامی پرسنل تأثیر مثبت داشته باشد.

---

۱. «تأثیر بازدارنده افشاگری پرسنل بر روی رصد مالی و رویکرد مالیاتی شرکت‌ها» از یارون وایلد (Jaron H. Wilde) برگرفته از مجله حسابداری *The Accounting Review*, 1 September 2017; 92 (5): 247–280. «مدیریت ریسک کلاهبرداری در کسب‌وکار: یک راهنمای اجرایی»، برگرفته از مؤسسه حسابرسان درونی، مؤسسه آمریکایی حسابداری عمومی، ص ۳۵.

چه کسانی باید سیستم‌های افشاگری درونی را راه‌اندازی کنند؟

همه سازمان‌های دولتی و خصوصی باید از سیستم افشاگری درونی برخوردار باشند.

همه سازمان‌های دولتی

تمامی نهادهای دولتی در سطوح محلی، منطقه‌ای، ملی و بین‌المللی بدون‌استثناء بایستی سیستم افشاگری درونی (IWS) را اجرایی نمایند و این راه‌اندازی البته بایستی براساس اندازه هر سازمان باشد.[1] این قاعده شامل نهادهایی که مالکیت دولتی دارند نیز می‌شود و شرکت‌های بازرگانی در کنترل دولت نیز بخشی از آن هستند.

خصوصی‌ترین سازمان‌ها[2]

- همه نهادهای خصوصی متوسط و بزرگ (با بیش از ۵۰ پرسنل) افزون بر تمامی نهادهای صنعت ارائه‌دهندگان خدمات مالی، صرف‌نظر از اندازه[3] بایستی IWS ایجاد کنند. این دامنه شامل شرکت‌ها و سازمان‌های غیرانتفاعی نیز می‌گردد.
- نهادهای خصوصی کوچک (با کمتر از ۵۰ پرسنل) به‌شدت برای به‌کارگیری IWS توصیه شده‌اند. به‌ویژه مؤسساتی که کارشان با ریسک منافع همگانی

---

۱. حتی شهرداری‌های کوچک نیز پیوسته در حال تصمیم‌گیری در حوزه‌های پرریسکی مانند خدمات عمومی، حفاظت از محیط‌زیست و بهداشت همگانی هستند. ازاین‌رو وجود IWS در آن‌ها ضروری است. قوانین اتحادیه اروپا به شهرداری‌ها اجازه می‌دهد کانال‌های افشاگری مشترک داشته باشند، بااین‌وجود هر یک از آن‌ها بایستی یک سیستم افشاگری در درون خود داشته باشد تا ابعاد دیگر سازمان نیز تحت پوشش قرار گیرد.

۲. سازمان‌های خصوصی ازجمله سازمان‌های حوزه سوم شامل مؤسسات غیرانتفاعی همچون مؤسسات مدنی، خیریه‌ها و مؤسسات غیردولتی.

۳. این امر به دلیل ریسک پولشویی و تأمین مالی تروریسم می‌باشد. بیشتر نهادهای خصوصی ارائه‌دهنده سرویس‌های مالی در حیطه اتحادیه اروپا به‌واسطه قوانین گوناگون این اتحادیه ملزم به راه‌اندازی IWS هستند.

همراه است (مانند ریسک حقوق بشر، محیط‌زیست و بهداشت همگانی). شرکت‌هایی که زیرمجموعه گروه‌های تجاری هستند نیز بایستی صرف‌نظر از اندازه شرکت، IWS را به‌کار بگیرند.[1]

- نهادهای خصوصی متوسط و کوچک (با کمتر از ۲۵۰ پرسنل) می‌توانند برای اشتراک‌گذاری منابع خود در راستای دریافت گزارش‌ها و رسیدگی‌های متعاقب نسبت به ایجاد IWS اقدام کنند. درعین‌حال، مسئولیت حفظ محرمانگی و دادن بازخورد به افشاگر و همچنین رسیدگی به تخلفات گزارش‌شده به‌صورت جداگانه متوجه هر نهاد می‌باشد.
- همه نهادهای خصوصی شامل آن‌هایی که سیستم افشاگری درونی ایجاد نکرده‌اند بایستی در برابر هرگونه رفتار آسیب‌زا از افشاگران حفاظت نمایند.

موارد اساسی در راه‌اندازی سیستم‌های افشاگری درونی

- هر سیستم افشاگری درونی بایستی متناسب با اندازه سازمان و میزان ریسک تخلف در آن ایجاد گردد. به این ترتیب سازمان‌ها بایستی ریسک‌ها و نیازهای خود را برآورد کرده و آگاهانه دست به طراحی IWS بزنند.
- IWS به بخشی از بستر اداره سازمان تبدیل می‌شود و در چاچوب برنامه‌های پاکدستی و قانون‌مداری و یا دست‌کم در پیوند با آن‌ها طراحی می‌شود. این سیستم‌ها با منابع انسانی (HR) و رویه‌های شکوائیه‌ها متفاوت هستند.[2]

---

۱. شرکت‌های کوچکی که زیرشاخه گروه‌های تجاری هستند، به‌سادگی می‌توانند به‌صورت مشارکتی از سیستم دریافت گزارش‌ها و رسیدگی به آن استفاده نموده و از IWSهایی در سطح گروهی بهره گیرند. مزایای به‌کارگیری این سازوکارها به‌مراتب از هزینه‌های اجرای IWS در سطح نهادهای کوچک بالاتر است.

۲. مراجعه شود به: «کانال‌های ارتباطی IWS و دیگر سیستم‌های گزارش‌دهی درونی» از فصل «چشم‌انداز».

- در طراحی IWS بایستی با همه طرف‌های مربوطه از همه سطوح چه در حوزه بیرونی و چه در حوزه درونی مشورت شود و در موارد لازم رضایت آنان جلب گردد. این طرف‌ها شامل پرسنل، شوراهای کار، اصناف و دیگر نمایندگان پرسنلی هستند.
- IWS بایستی در راستای مقتضیات قوانین کشوری طراحی شود. ازجمله مقررات حفاظت از افشاگر و دیگر قوانین مربوطه مانند قوانین حفاظت از داده و قانون کار.
- ساختار IWS بایستی فراگیر بوده و نسبت به جنسیت حساس باشد.[1]

دستور کارهای حفاظت از افشاگر در اتحادیه اروپا

در سال ۲۰۱۹ اتحادیه اروپا، دستور کار ۲۰۱۹/۱۹۳۷ پارلمان اروپا و دستور کار ۲۳ اکتبر ۲۰۱۹ شورای اروپا در زمینه حفاظت از افرادی که تخلف از قوانین اتحادیه را گزارش می‌دهند، برای اجرا به تصویب رساند. ۲۷ عضو اتحادیه اروپا به‌مدت دو سال تا سپتامبر ۲۰۲۱ فرصت داشتند برای اجرایی کردن این قوانین که به «دستور کار حفاظت از افشاگر» مشهور هستند آماده شوند. بیشتر کشورها تا سررسید اجرای این قانون فاقد آمادگی لازم بودند.[2]

مجموعه این دستور کار، حداقل استانداردهای موردنیاز برای حفاظت از افشاگران در اروپا را شرح می‌دهد. کشورهای عضو بایستی محتوای این قانون را بر اساس روح دستورکار که چیزی جز بالاترین سطح حفاظت از افشاگران نیست، برای خود اولویت‌بندی نمایند.

---

۱. مراجعه شود به «بلند کردن صدا، یافتن عدالت: موانع زنان در راه گزارش دادن فساد در اتحادیه اروپا» (۲۰۲۱) از شفافیت بین‌الملل. «حساست جنسی در افشاگری و گزارش‌دهی فساد» (۲۰۲۰) از نیوز زونیگا (Nieves Zúñiga).

۲. مراجعه شود به رصد افشاگری اتحادیه اروپا در راستای ارزیابی پیشرفت دستورکار افشاگری اتحادیه اروپا در میان ۲۷ کشور عضو این اتحادیه به آدرس: www.whistleblowingmonitor.eu

بندهای اساسی دستورکار افشاگر اتحادیه اروپا

- این دستورکار هر دو بخش خصوصی و دولتی را پوشش می‌دهد.
- دستورکار دامنه گسترده‌ای از افشاگران ازجمله افراد بیرون از چارچوب پرسنلی را پوشش می‌دهد؛ مانند مشاوران، پیمانکاران، داوطلبان، اعضای هیئت‌ها، کارکنان پیشین و درخواست‌کنندگان کار (ماده ۴).
- این دستور کار از کسانی که افشاگران را یاری می‌کنند حفاظت کرده و افراد یا نهادهای حقیقی و حقوقی مربوط به افشاگر را زیر پوشش خود می‌گیرد (ماده ۴-۴).
- نقض مقررات عبارت است از کنش یا بی‌کنشی که خلاف قوانین باشد و یا در مقابل هدف و منظور قوانین باشد (ماده ۵-۱).
- این دستورکار قانونی در زمینه قرار دادن افشاگر زیر چتر حفاظتی به‌هیچ عنوان انگیزه وی برای گزارش‌دهی را لحاظ نمی‌کند.
- دستورکار در بیشتر موارد از هویت افشاگر نگهداری کرده و موارد استثنای این محرمانگی محدود و شفاف هستند. در مواردی که نیاز است هویت افشاگر آشکار شود، از پیش به آگاهی وی رسانده خواهد شد (ماده ۱۶).
- این دستورکار از کسانی که به‌طور ناشناس اطلاعاتی را گزارش داده یا آشکار کرده و پس از آن شناسایی شده‌اند، حفاظت می‌کند (ماده ۶-۳).
- برمبنای این دستور کار دامنه گسترده‌ای از نهادهای دولتی و خصوصی وظیفه دارند، سیستم افشاگری درونی را راه‌اندازی نمایند (ماده ۸).
- نهادهای دولتی و خصوصی و همچنین مقامات مربوطه موظف‌اند گزارش‌های دریافتی را پیگیری نموده و افشاگر را در بازه زمانی مقتضی آگاه نگه دارند (مواد ۹ و ۱۱-۲).

- افشاگران مجازند نقض قانون را بـه شـکل درونـی و یـا مسـتقیماً بـه مقامـات مربوطه اطلاع دهند (ماده ۱۰).
- دستورکار در برخی موارد اجازه می‌دهد اطلاعات بـرای همگـان منتشـر شـود (ماده ۱۵).
- هرگونه تلافی مانند تهدید به تلافی و تلاش برای آن ممنوع بوده و یـک لیسـت متنوع و غیرفراگیر از نمودهای آن در قانون پیش‌بینی شده است (ماده ۱۹).
- دستورکار کشورهای عضو اتحادیه اروپا را ملزم می‌دارد مشـاوره‌های رایگـان، فراگیر و مستقل را در اختیار همگان قرار دهند (ماده ۲۰-۱الف).
- در دستورکار، کمک‌های مالی و قانونی گوناگونی برای افشـاگر در نظـر گرفتـه شده که مؤلفه‌های مهمی در حفاظت کارآمـد از افشـاگر محسـوب می‌شـوند (ماده ۲۰-۲).
- درصورتی‌که افشاگر آسیب ببیند، دستورکار فرض را بر تلافی می‌گذارد (مـاده ۵-۲۱).
- دستورکار برای افشاگر کمک‌های موقتی را در نظر گرفته بـا ایـن هـدف کـه تـا زمان اتمام رسیدگی حقوقی، افشاگر بتواند جایگاه حرفه‌ای و مالی خـویش را حفظ کند (ماده ۲۱-۶).
- برای کسانی که مانع گزارش‌دهی شوند، برای آن مشکل ایجاد کنند، بـه قصـد تلافی برآیند (ازجمله با پیگردهای قانونی آزاردهنده) یا در وظیفه خـود بـرای حفظ محرمانگی هویت افشاگر کوتاهی کننـد، مجازات‌هـایی در نظـر گرفتـه شده است (ماده ۲۳).
- با توجه به مفاد دستورکار، امکان مسئول دانستن افشاگران در قبال نقض قوانین مربوط به دسترسی و افشای اطلاعات وجود نـدارد و ایـن نقـض محرمـانگی

اسرار تجاری نیز از این قاعده جدا نیست (ماده ۲۱ (۲-۳-۷)). همچنین امکان جلوگیری از افشای اطلاعات به‌وسیله قرارداد (مانند بندهای وفاداری، رازداری یا عدم افشای اطلاعات) وجود ندارد (ماده ۲۴).

مبانی اصلی سیستم‌های افشاگری درونی

همه سازمان‌های دولتی و خصوصی می‌بایست بر اساس مبانی زیر یک سیستم افشاگری درونی راه‌اندازی نمایند:

چشم‌انداز

۱. سیستم‌های افشاگری درونی باید پذیرای گزارش‌های مربوط به تخلفات احتمالی باشند. این تخلفات شامل هرگونه فعل یا ترک‌فعل خلاف قانون، سوءاستفاده‌گرایانه یا آسیب‌زننده از سوی سازمان یا در چارچوب آن باشند.

۲. سیستم‌های افشاگری درونی باید پذیرای گزارش‌های رسیده از افرادی باشند که در محیط کار خود به اطلاعاتی در زمینه تخلف یا کم‌کاری توسط سازمان یا برای سازمان دست پیدا کرده‌اند.

۳. سازمان‌ها برای حفاظت از افشاگران وظیفه دارند. سازمان باید از هر فرد یا افرادی که مسائلی درباره گمان تخلف ارائه نموده، حفاظت کرده و درعین‌حال به‌لحاظ منطقی استدلال کنند که اطلاعات گزارش‌شده می‌تواند در چارچوب زمان و شرایط درست باشد. سازمان‌ها همچنین در قبال حفاظت از طرف‌های سوم در برابر هرگونه اقدام آسیب‌زا دارای مسئولیت هستند.

نقش‌ها و مسئولیت‌ها

۱. رأس مدیریت هر سازمان برای پیاده‌سازی کارآمد IWS در سازمان خود مسئول و پاسخ‌گو می‌باشد. مدیران اصلی هر سازمان می‌توانند با پشتیبانی شفاف از بالا به پایین و استقبال از گفت‌وشنود مسائل مربوط به تخلف، پایبندی خود را به این مسئولیت‌ها نشان دهند.

۲. سازمان‌ها بایستی یک فرد یا دپارتمان بی‌طرف را مسئول راه‌اندازی سیستم افشاگری درونی خود نمایند. این فرد یا دپارتمان نباید در حیطه تضاد منافع قرار گیرد و افزون بر داشتن شرایط لازم از اختیارات و منابع مستقل کافی بهرمند گردد.

اطلاعات و ارتباطات

۱. اطلاعات IWS در هر سازمان باید در میان دامنه گسترده‌ای از کانال‌ها و رسانه‌ها، بسیار آشکار و قابل دسترسی باشد. همه طرف‌های دخیل ازجمله افشاگران احتمالی و دیگر افراد مربوطه بایستی به اطلاعات سیستم افشاگری درونی دسترسی داشته و آن‌ها را دریافت کنند.

۲. سازمان‌ها وظیفه دارند در راستای پایبندی به عبارت «گفت‌وشنود» در مقررات تعریف‌شده برای IWS، هر ساله بر تعهد خود نسبت به اجرای این سیستم و فرهنگ آن تأکید نمایند.

سازوکارها

۱. سیستم‌های افشاگری درونی باید دارای چند کانال گزارش‌دهی گوناگون باشند. این کانال‌ها بایستی به‌سادگی در دسترس، امن و برخوردار از امکان انتقال شفاهی و کتبی باشند. سازمان‌ها بایستی سرپرست‌های بخش‌های

زیرمجموعه خود را به‌عنوان گیرنده احتمالی گزارش‌های افشاگری در نظر داشته باشند.

۲. هر سیستم افشاگری درونی باید ضامن پیگیری پرتلاش همه گزارش‌های دریافتی باشد.[۱] به‌عبارت‌دیگر، پیگیری گزارش‌ها بایستی تمام و کمال، در بازه زمانی مناسب، عادلانه و بی‌طرفانه انجام پذیرد. هدف از این کار مشخص کردن این مسئله است که آیا تخلف صورت گرفته[۲] یا خیر و با تأیید تخلف به آن رسیدگی شده و هر مسئله سیستمی مربوط به آن شناسایی شود و مشکلات به‌وجودآمده برطرف گردد. پیگیری گزارش‌ها بایستی با مشارکت معنادار افشاگر دنبال شود.

۳. افشاگران به‌عنوان طرف‌های آشنا و متمایل به موضوع بایستی در حین فرایند رسیدگی به گزارش‌ها از مسائل آگاه شده و برای ارائه دیدگاه‌های خود در راستای رسیدگی به گزارش از فرصت‌های مناسب بهرمند گردند.

۴. گزارش‌های دریافتی، اقدامات انجام‌شده برای پیگیری، یافته‌ها و خروجی پیگیری به‌همراه ارتباطات صورت‌گرفته با افشاگران و افراد دخیل باید به شکل مناسب مستند گردد و با توجه به محرمانگی و مقتضیات حفاظت از داده به‌گونه‌ای بایگانی شوند که امکان بازیابی و بازرسی آن‌ها محفوظ باشد.

پشتیبانی و حفاظت از افشاگران

۱. بدون رضایت صریح افشاگر، اطلاعات مربوط به هویت وی نباید جز برای افراد صلاحیت‌دار دریافت‌کننده یا پیگیر گزارش‌ها آشکار گردد. این قاعده

---

۱. ازجمله گزارش‌هایی که به‌صورت ناشناس فرستاده شده‌اند.

۲. یا تخلفی که ممکن است صورت پذیرد.

شامل هرگونه اطلاعاتی است که ممکن است هویت افشاگر به شکل مستقیم یا غیرمستقیم از آن‌ها برداشت شود.

۲. سازمان‌ها وظیفه دارند گزارش‌های ناشناس را دریافت و پیگیری نموده و از افشاگران ناشناس حفاظت نمایند.

۳. سازمان‌ها وظیفه دارند هرگونه رفتار آسیب‌زا ازجمله تهدید، پیشنهاد، فعل و یا ترک‌فعل مستقیم یا غیرمستقیم که ممکن است برای افشاگر (یا افراد مرتبط با وی) زیان یا آسیب به‌همراه داشته باشد را ممنوع ساخته و از هرگونه مداخله در افشاگری توسط طرف‌های مربوطه جلوگیری کنند.

۴. سازمان‌ها وظیفه دارند در راستای پیشگیری از اقدامات آسیب‌زا و تضمین خودداری افراد و نهادهای زیر امرشان از هرگونه رفتار آسیب‌زا، اقدامات مناسب و منطقی را اتخاذ نمایند.

۵. سیستم‌های افشاگری درونی بایستی دارای سازوکارهای اجراپذیر، شفاف و زمان‌بندی شده‌ای باشند تا (۱) هر شکایت از رفتار آسیب‌زا، مداخله و نقض محرمانگی دریافت و پیگیری شود؛ (۲) دست‌اندرکاران تخلف بازخواست گردند و (۳) افشاگران و دیگر افراد حفاظت‌شده‌ای که متحمل رنج شده‌اند، به‌طور کامل مورد رسیدگی و بهبود قرار گرفته و اقدامات لازم برای جبران زیان‌های وارده به آنان صورت پذیرد.

۶. سازمان‌ها وظیفه دارند با پشتیبانی از افشاگران خود از هرگونه آسیب به سلامت و حرفه آنان جلوگیری نمایند.

حفاظت از افراد دخیل

سازمان‌ها وظیفه دارند از هویت و حقوق افراد دخیل در افشاگری حراست کنند و در این راستا برای کسانی که دانسته اطلاعات نادرستی را گزارش می‌کنند، مجازات‌های متناسب و بازدارنده در نظر بگیرند.

رصد و ارزیابی پیوسته

سیستم‌های افشاگری درونی باید دست‌کم هر سال موردارزیابی قرار گیرند و برمبنای آن تدابیری در جهت بهبود کارایی این سیستم‌ها و همخوانی آن‌ها با آخرین مقررات و رویکردهای اجرایی اندیشیده شود.

دامنه

هر سازمان باید به‌روشنی مشخص کند که چه کسانی می‌توانند در چارچوب IWS گزارش دهند، چه چیزهایی را می‌توانند گزارش دهند و چه کسانی مورد حفاظت قرار می‌گیرند.

انواع تخلفات زیر پوشش سیستم‌های افشاگری درونی

سیستم‌های افشاگری درونی بایستی هرگونه گزارش در زمینه گمان بروز تخلف در سازمان یا توسط آن را پذیرا باشند.

- تخلف بایستی هرگونه فعل یا ترک‌فعلی تلقی گردد که خلاف قانون، سوءاستفاده یا آسیب زننده می‌باشد. تخلف موارد زیر را دربر می‌گیرد اما به آن‌ها محدود نمی‌شود:
  - فساد در همه شکل‌های آن (مانند رشوه‌خواری، پولشویی و اخاذی جنسی)؛

- تخلفات کیفری؛
- نقض تعهدات حقوقی (ملی و بین‌المللی)؛
- خطرآفرین برای همگان، بهداشت شغلی و ایمنی شغلی؛
- خطرآفرین برای محیط‌زیست؛
- نقض حقوق بشر؛
- بهره‌کشی یا سوءاستفاده از کودکان؛
- آزار جنسی، زورگویی و تبعیض؛
- سوءاستفاده، کوتاهی یا بی‌رحمی در قبال حیوانات؛
- ایجاد انحراف در تحقق عدالت؛
- سوءاستفاده از قدرت؛
- دادوستد درون‌سازمانی، فرار مالیاتی یا نقض قوانین ممنوعیت تشکیل اتحادیه و نقض تحریم‌های بازرگانی بین‌المللی؛
- استفاده بدون‌مجوز از منابع مالی، دارایی‌ها و دیگر منابع؛
- هدر دادن یا سوءمدیریت؛
- تضاد منافع؛
- افشای مسائل مالی برای کلاهبرداری؛
- رفتار آسیب‌زا در برابر افشاگران و دیگر طرف‌های حفاظت‌شده؛
- رفتار نامناسبی که می‌تواند به اعتبار یا جایگاه اقتصادی سازمان لطمه وارد کند؛
- هرگونه تخلف از آیین‌نامه‌های سازمانی، آیین‌نامه‌های اخلاقی و سیاست‌های موجود در این حوزه؛

- پنهان کردن یا تلاش برای پنهان کردن تخلف، ازجمله مانع شدن یا تلاش برای مانع تراشی بر سر راه افشاگری.

- موارد نقض قرارداد شخص افشاگر با سازمان ازقبیل نقض قرارداد کار، قرارداد مشاوره، قرارداد پیمانی و مواردی از این دست در دامنه تخلفات قابل گزارش به‌وسیله IWS محسوب نمی‌شود، جز در مواردی که گزارش تخلف شامل موارد تعریف شده در قوانین فوق باشد. این گزارش‌ها و به‌طورکلی تمامی شکایت‌های مربوط به تخلف در دیگر سیستم‌های سازمانی همچون پروسه شکایت منابع انسانی مورد رسیدگی قرار می‌گیرند (توضیحات مربوطه در ادامه و در بخش «کانال‌های ارتباطی IWS و دیگر سیستم‌های گزارش‌دهی درونی» آمده است).
- IWS بایستی پذیرای گزارش‌های حاوی موارد ظن تخلف از سوی همه کسانی باشد که مستقیم یا با واسطه برای سازمان کار می‌کنند و یا دارای هرگونه قرارداد یا پیمان با سازمان هستند. کسانی که در این دامنه جای دارند عبارت‌اند از: کارکنان کنونی و پیشین، پرسنل اجرایی، اعضای هیئت‌مدیره، کارآموزان، دانشجویان در حال کار، داوطلبان، پیمانکاران، پیمانکاران زیرمجموعه، تأمین‌کنندگان، مشاوران و هر فرد دیگری که درون‌سازمان یا برای آن فعالیت دارد.
- IWS بایستی پذیرای گزارش‌های مربوط به ظن تخلفاتی باشد که رخ داده، در حال انجام هستند یا احتمال انجام‌شان وجود دارد.
- IWS حق ندارد گزارش‌های حاوی اطلاعاتی ازقبیل اسرار تجاری سازمان یا اطلاعات مالی منتشرنشده را مورد رسیدگی قرار دهد.

- سازمان‌هایی که با مسائلی همچون امنیت ملی، اسرار اداری یا نظامی و اطلاعات طبقه‌بندی‌شده سروکار دارند نباید گزارش‌هایی که به این موارد مربوط هستند را از IWS بگیرند. این سازمان‌ها می‌توانند کانال‌های ویژه‌ای ایجاد کرده و گزارش‌های حاوی اطلاعات مربوط به امنیت ملی، اسرار اداری یا نظامی یا اطلاعات طبقه‌بندی‌شده را از این کانال‌ها دریافت نموده و پرسنل واجد شرایط را برای اداره این سازوکار بگمارند.

کانال‌های ارتباطی بین IWS و دیگر سیستم‌های گزارش‌دهی درونی

معمولاً در سازمان‌ها به‌جز سیستم افشاگری درونی، سیستم‌های گزارش‌دهی و ثبت شکایت دیگری نیز وجود دارد. این سیستم‌ها به‌طورکلی به شکایت‌های پرسنلی و کاری درون‌سازمانی رسیدگی می‌کنند. کانال‌های ارتباطی بین این سیستم‌ها ممکن است با مشکلاتی همراه باشد، به‌ویژه در مواردی که دامنه کاری سیستم‌ها با یکدیگر همپوشانی دارد. برای نمونه گاهی رسیدگی به گزارش‌های آزار، تبعیض، حفاظت از داده، سلامت شغلی، تخلفات ایمنی و مواردی از این دست با پیچیدگی‌هایی همراه‌اند و چندگونه تخلف را دربرمی‌گیرند. افزون‌براین، بسته به دامنه و نوع سیستم گزارش‌دهی و ثبت شکایت در هر سازمان، مسائلی مانند رویکردها و شیوه‌های تحقیقات، حقوق و تعهدات سازمان و فرد گزارش‌دهنده ممکن است در زمینه رسیدگی، منشاء بروز اختلافاتی شوند.

- سازمان‌ها بایستی با ارائه مجموعه‌ای از رهنمودها، مشخص نمایند که برای هر نوع گزارش یا شکایت، چه سیستم دریافت و پیگیری مناسب‌تر است. از سوی دیگر، فراهم کردن دسترسی به اطلاعات شفاف به کمک ابزارهایی مانند

«پرسش‌های رایج» در کنار افزایش آگاهی پرسنل می‌تواند زمینه رفتن افراد به سراغ کانال‌های گزارش‌دهی مناسب باشد.

- سازمان‌ها نباید در زمینه برگزیدن کانال‌ها ارتباطی از سوی افراد، رویکرد جزئی داشته باشند و سخت‌گیری کنند چراکه افراد را از ابزار دغدغه‌هایشان دور می‌کند؛ به‌طوری‌که، گزینش کانال ارتباطی باید برعهده طرف گزارش‌دهنده باشد.
- اگر پس از ارزیابی اولیه مشخص شود که یک سیستم گزارش‌دهی یا ثبت شکایت دیگر برای مورد ارزیابی شده مناسب‌تر است، بهتر است فرد گزارش‌دهنده برای ارائه گزارش یا شکایت خود در کانال مناسب‌تر راهنمایی گردد. گزارش‌ها نباید برای افراد یا دپارتمان‌های فعال در دیگر سیستم‌های گزارش‌دهی فرستاده شوند مگر آنکه فرد نگارنده گزارش به صراحت رضایت خود را از این کار ابراز نماید.
- گزارش‌هایی که بافت ترکیبی یا دامنه مبهم دارند، بایستی در چارچوب سیستم برگزیده فرد گزارش‌دهنده مدیریت شوند و در صورت نیاز با دیگر سیستم‌های مربوطه هماهنگی لازم صورت گیرد.

کسانی که باید امکان گزارش‌دهی با سیستم افشاگری درونی را دارا باشند

سیستم‌های افشاگری درونی باید پذیرای گزارش‌های کسانی باشند که ممکن است در چارچوب فعالیت‌های کاری خود به اطلاعاتی در زمینه تخلف در سازمان یا از سوی سازمان دست پیدا کنند.

- عمده کسانی که واجد شرایط استفاده از IWS هستند، صرف‌نظر از اینکه همکاری‌شان با سازمان در جریان است یا به اتمام رسیده، در زیر دسته‌بندی شده‌اند:
  - کارکنان (شامل کارکنان تمام‌وقت، پاره‌وقت، دوره‌ای یا موقت) ازجمله پرسنل دولتی؛
  - افراد خوداشتغال؛
  - سهامداران و افراد فعال در بدنه اداری، مدیریتی یا سرپرستی؛
  - داوطلبان مزدبگیر و کارآموزان بی‌مزد؛
  - کسانی که زیرمجموعه سرپرستی، پیمانکاری، پیمانکاران فرعی و تأمین‌کنندگان کار می‌کنند؛
  - کسانی که در حین فرایند استخدام یا در دوره مذاکرات عقد قرارداد (مانند زمان پرکردن فرم‌های اشتغال سازمان) به اطلاعاتی دست پیدا می‌کنند.
- سیستم‌های افشاگری درونی سازمان‌ها همچنین باید اطلاعات ارائه‌شده درباره تخلف سازمان یا تخلف در سازمان، از سوی تمامی طرف‌های مربوط به فعالیت‌های خود را در نظر بگیرند. کاربران، مشتریان، بهره‌برداران و ساکنان محلی در این زمینه واجد شرایط هستند. از سوی دیگر سازمان‌ها می‌توانند برای ایجاد سیستم‌های جداگانه‌ای با هدف رسیدگی به گزارش‌های رسیده از بیرون اقدام نمایند.
- پیرامون تصمیم‌گیری درباره دسته‌بندی کسانی که می‌توانند به‌وسیله IWS گزارش دهند (ازجمله کارکنان، داوطلبان، پرسنل پیمانکاران فرعی، کاربران و بهره‌برداران) سازمان‌ها بایستی در مشخص کردن دسته‌بندی افراد و انواع رفتارهای آسیب‌زایی که ممکن است متوجه آن‌ها باشد و چگونگی حفاظت و

پشتیبانی از این افراد دقت‌نظر لازم را لحاظ نموده و اطلاعات شفافی را در این رابطه در اختیار گزارش‌دهندگان قرار دهند.

کسانی که مورد محافظت قرار می‌گیرند

سازمان‌ها وظیفه دارند از افشاگران حفاظت نمایند. این حفاظت از یک‌سو متوجه کسانی است که اطلاعاتی درباره موضوعی که احتمال تخلف در آن وجود دارد، گزارش کرده و به‌لحاظ منطقی گزارش آن‌ها در بازه زمانی مورد نظر می‌تواند درست باشد و از سوی دیگر متوجه طرف‌های سومی است که ریسک رفتار آسیب‌زا در قبال آن‌ها وجود دارد.

افشاگران

- افشاگر به کسانی گفته می‌شود که اطلاعاتی در زمینه موضوعی که احتمال تخلف در آن وجود دارد، ارائه کرده و به‌لحاظ منطقی اطلاعات آن‌ها در زمان موردنظر درست است؛
- منظور از «به‌لحاظ منطقی» آن است که اطلاعات ارائه‌شده از سوی فردی که دانش، تحصیلات و تجربه لازم را دارد مورد تأیید باشد. سازمان‌ها وظیفه دارند صرف‌نظر از اینکه درنتیجه تحقیقات تخلفی شناسایی می‌شود یا خیر؛ از افشاگران حفاظت کنند. این حفاظت شامل کسانی که درنتیجه خطای صادقانه اطلاعات نادرستی گزارش نموده‌اند نیز می‌شود. به‌ندرت اتفاق می‌افتد افشاگر در جایگاهی باشد که از تمامی ماجرا به‌خوبی آگاهی داشته باشد؛ ازاین‌رو برخی دیدگاه‌های افشاگران ممکن است درست نباشد.
- سازمان‌ها بایستی بدون در نظر گرفتن انگیزه‌های گزارش‌دهی از افشاگران حفاظت کنند.

- سازمان‌ها وظیفه دارند صرف‌نظر از اینکه افشاگران به مسئولان دورن‌سازمانی یا بیرون از سازمان گزارش داده‌اند یا گزارش آن‌ها انتشار پیدا کرده است از فرد افشاگر حفاظت نمایند.
- سازمان‌ها وظیفه دارند از کسانی که به شکل ناشناس افشاگری کرده و سپس هویت‌شان آشکار می‌شود، حفاظت کنند.
- سازمان‌ها بایستی صرف‌نظر از اینکه افشاگر از کانال‌های مشخص درون‌سازمانی استفاده کرده یا به مسئولان درونی بی‌طرف (مانند مدیران، مسئولان سلامت و ایمنی، سرپرست امور رسیدگی به شکایات، مسئول بخش منابع انسانی، مسئول کمیته سلامت اداری، مسئول حقوقی یا امور مربوط به بخش خصوصی، مسئول مالی، سرپرست دایره بازرسی یا عضو هیئت‌مدیره) گزارش داده باشد، از وی محافظت کنند. این حفاظت همچنین شامل کسانی می‌شود که گزارش تخلف را در چارچوب وظایف کاری خود ارائه نموده‌اند.

اشخاص ثالثی که در خطر رفتار آسیب‌زا قرار دارند

- کسانی که باور یا گمان افشاگری آن‌ها وجود دارد؛ حتی به اشتباه؛
- مؤسسات حقوقی که افشاگر صاحب آن‌هاست، در آن‌ها کار می‌کند و یا با آن‌ها ارتباط دارد؛
- طرف‌های سومی که با افشاگر رابطه دارند؛ همچون همکاران و خویشاوندان؛
- اشخاص بی‌طرفی که به افشاگر کمک کرده یا برای کمک به وی تلاش نموده‌اند؛
- اشخاص حقوقی ازجمله سازمان‌های مدنی و اتحادیه‌های بازرگانی که به افشاگر کمک کرده یا برای کمک به وی تلاش نموده‌اند؛

- کسانی که نام آن‌ها در گزارش به‌عنوان شاهد بالقوه آمده است؛
- کسانی که در پیگیری گزارش شرکت دارند (مانند شاهدان)؛
- کسانی که از مشارکت در تخلف خودداری نموده‌اند.

نقش‌ها و مسئولیت‌ها

نقش‌ها و مسئولیت‌های همه افراد درگیر در پیاده‌سازی سیستم افشاگری درونی بایستی به‌روشنی مشخص شده و بیان گردد.

رأس مدیریت

راس هرم مدیریت سازمان برای اجرای کارآمد IWS مسئول و پاسخ‌گو می‌باشد. آن‌ها بایستی پایبندی و پشتیبانی «از بالا به پایین» خود از بیان و دریافت موارد تخلف را آشکارا نشان دهند.

- رهبری سازمان می‌تواند مقام ریاست، عضو هیئت‌مدیره، سرپرست کل یا مدیر ارشد سازمان باشد. وی موظف است در قبال تعهدات درون‌سازمانی و عمومی خود نسبت به اجرای IWS رویکرد آشکار خود را به شیوه «از بالا به پایین» در سلسله‌مراتب سازمان نشان دهد. وی همچنین مسئول ایجاد و حفظ فرهنگ «بیان و رسیدگی» در سرتاسر سازمان است.
- سیستم‌های افشاگری درونی باید از سوی رأس مدیریت هر سازمان تأیید شده و توسط هیئت‌مدیره یا همتای آن معتبر شناخته شود.
- هیئت‌مدیره یا همتای آن بایستی مسئولیت کلی IWS را بر دوش رئیس سازمان بگذارد. درمقابل، رئیس سازمان، ابعاد اجرایی این سیستم را در قالب مأموریت به مسئول افشاگری یا سرپرست دایره افشاگری واگذار می‌کند.

- هیئت‌مدیره یا همتای آن به‌همراه رئیس سازمان بایستی ضامن دسترسی IWS به منابع کافی و کارکرد کارآمد این سیستم باشند.
- هیئت‌مدیره یا همتای آن وظیفه دارند نظارت دقیقی روی IWS داشته و آن را پاسخ‌گو نمایند. به این منظور می‌توان از رئیس سازمان، سرپرست دایره افشاگری و مسئول افشاگری از نحوه طراحی و کار IWS پرس‌وجو شود.
- اعضای هیئت‌مدیره، رئیس سازمان و مدیران ارشد باید آموزش‌های لازم را در زمینه IWS ببینند.

مسئول یا دایره افشاگری

سازمان‌ها وظیفه دارند فرد یا دپارتمان بی‌طرفی را مسئول اجرای IWS نمایند. این فرد یا دپارتمان بایستی فارغ از تضاد منافع بوده و از استقلال، اختیارات، منابع و ویژگی‌های کافی برخوردار باشد.

- باتوجه به اندازه سازمان، ریسک و نیازهای موجود در هر سازمان باید یک فرد (که «مسئول افشاگری» نامیده می‌شود) یا دپارتمان (که «دایره افشاگری» نامیده می‌شود) مسئول اجرای سیستم افشاگری درونی شده و مسئولیت‌های زیر را برعهده بگیرد:
  - قرار دادن اطلاعات مربوط به سازوکار افشاگری و حفاظت از افشاگر سازمان در اختیار هرکسی که خواهان دانستن آن باشد؛
  - دریافت کردن گزارش‌ها؛
  - پیگیری گزارش‌ها؛
  - حفظ ارتباط با افشاگران ازجمله درخواست اطلاعات بیشتر از آن‌ها در موارد ضروری و دادن بازخورد به آن‌ها؛

- طراحی، نظارت و ارزیابی سیستم افشاگری درونی؛
- گزارش‌دهی مستمر به رئیس سازمان و اعضای هیئت‌مدیره از امور اجرایی IWS؛

- مسئول یا اداره افشاگری بایستی بی‌طرف باشد؛ بدین‌معنا که هیچ تضاد منافعی نداشته و از استقلال کافی برخوردار باشد. رعایت این مسئله به ساختار سازمانی، ساختاری اداره سازمان و شیوه‌نامه‌های هر سازمان برمی‌گردد که چگونگی آن‌ها به اندازه سازمان و سطح منابع در درسترس آن بستگی دارد.
  - مسئول افشاگری یا سرپرست دایره افشاگری باید به هیئت‌مدیره یا همتای آن که ناظر بر کار IWS است، دسترسی آسان داشته باشد. به‌منظور تضمین این دسترسی، مسئول افشاگری یا سرپرست دایره افشاگری بهتر است پیوسته و مستقیم به اعضای هیئت‌مدیره و ریاست سازمان گزارش دهد.
  - سیستم افشاگری درونی باید راه‌کارهایی برای حل مسائل تضاد منافع مسئول یا سرپرست افشاگری داشته باشد. برای نمونه باید سازوکارهایی برای رسیدگی به گزارش‌های افشاگری مربوط به سرپرست افشاگری یا دایره افشاگری در سازمان ایجاد گردد.
- مسئول افشاگری یا سرپرست دایره آن باید از منابع و اختیارات موردنیاز برای انجام وظایف خود در سطح کارآمد برخوردار باشد.
- بسته به اندازه و نیازهای هر سازمان، مسئول افشاگری آن می‌تواند افزون بر این مسئولیت، کارکردهای دیگری را نیز برعهده بگیرد. در این موارد:

- سازمان بایستی به‌طور مشخص به حجم کاری این مسئولان توجه داشته باشد تا آن‌ها بتوانند به نقش خود به‌عنوان مسئول افشاگری، زمان لازم را اختصاص دهند.
- بهتر است مسئول افشاگری در سلسله مراتب مدیریتی نباشد.

- مسئول افشاگری و اعضای دایره افشاگری باید صلاحیت‌های لازم را دارا بوده و به شکل پیوسته در زمینه اجرای سیستم افشاگری درون‌سازمانی آموزش ببینند. در این زمینه شایسته‌سالاری باید رعایت گردد.
- مهم است که افراد مسئول رسیدگی به گزارش‌ها از دید دیگران مورد اعتماد باشند؛ ازاین‌رو هر سازمان باید در گزینش افراد به معیارهای تنوع و فراگیری توجه نماید.

مدیران سلسله‌مراتبی

- مدیران سلسله‌مراتبی نیز باید در جایگاه دریافت‌کننده گزارش‌های افشاگری قرار داده شوند، چراکه آن‌ها طبیعی‌ترین و رایج‌ترین کانال‌ها برای گزارش دادن مسائل کاری در زندگی روزمره هستند.
- سازمان‌ها باید مدیران سلسله‌مراتبی خود را در زمینه دریافت و رسیدگی به گزارش‌های افشاگری و همچنین مدیریت مسائل به وجود آمده آموزش دهند. سرفصل‌های این آموزش‌ها عبارت‌اند از:
  - شناسایی گزارش‌های افشاگری؛
  - دامنه سیستم افشاگری درونی و بستر حقوقی آن؛
  - نحوه رسیدگی به اطلاعات دریافت شده و رعایت مسائلی همچون حفظ محرمانگی، حفاظت از داده و مستندسازی؛

- نقش‌گیرنده اطلاعات به‌عنوان شنونده و ارائه بازخورد.

این آموزش‌ها باید به‌صورت پیوسته انجام شود و می‌تواند درون‌سازمانی یا بیرون از آن باشد.

پرسنل

- هرگونه درگیر شدن پرسنل در رفتارهای آسیب‌زا نسبت به افشاگر یا طرف‌های سوم حفاظت‌شده به هر شکلی ممنوع می‌باشد.
- درصورتی‌که به‌جای کانال‌های گزارش‌دهی مشخص شده، یک گزارش از کانال‌های دیگری دریافت شود و یا به‌دست کسانی به‌جز مسئولان رسیدگی به گزارش‌ها برسد، آنگاه پرسنل دریافت‌کننده حق ندارند هرگونه اطلاعاتی که می‌تواند هویت افشاگر یا افراد مربوطه را آشکار نماید، را افشاء کنند. این پرسنل وظیفه دارند افشاگر را مستقیماً به کانال‌های مناسب راهنمایی کنند.
- سازمان‌ها بایستی پرسنل خود را از مسئولیت‌هایی که در قبال IWS دارند آگاه نمایند. در این راستا بهتر است از آموزش‌های آگاهی‌سازی استفاده شود.

اطلاعات و ارتباطات

تدابیر موردنیاز در زمینه اطلاعات و ارتباطات کلید آگاهی‌بخشی به همه طرف‌ها و پاسخ‌گو نمودن آن‌ها در زمینه IWS می‌باشد.

اطلاعاتی که باید در اختیار همه طرف‌های مربوطه گذارده شود

اطلاعات مربوط به IWS در هر سازمان باید به کمک طیف گسترده‌ای از رسانه‌ها و کانال‌ها به شکل بسیار روشن در دسترس قرار گیرد. همه طرف‌های مربوطه ازجمله

افشاگران احتمالی و افراد مرتبط با آن‌ها باید به اطلاعات مربوط به IWS دسترسی داشته باشند.

اطلاعاتی که باید فراهم باشد

سازمان‌ها وظیفه دارند اطلاعات شفاف و فراگیری را با دسترسی آسان در اختیار طرف‌های دخیل قرار دهند. این اطلاعات باید شامل موارد زیر باشند:

- تعهد مدیریت سازمان شامل رئیس سازمان، اعضای هیئت‌مدیره و مدیران ارشد به ایجاد فرهنگ «گفتن و شنیدن» در زمینه IWS؛ ازجمله تعهد نسبت به حفاظت از افشاگران، اقدام کردن در واکنش به دریافت گزارش‌های افشاگری و آموزش مدیران و پرسنل مربوطه؛
- چگونگی نظارت و پاسخ‌گو نمودن دست‌اندرکاران IWS از سوی هیئت‌مدیره؛
- سیاست‌ها و شیوه‌های سازمان در زمینه افشاگری و حفاظت از افشاگر که موارد زیر را در بر می‌گیرد:
  - دامنه IWS ازجمله در ارتباط با دیگر سیستم‌های گزارش‌دهی درونی؛
  - شرایط موردنیاز برای حفاظت از افشاگران؛
  - اطلاعات تماس برای اطلاعات درون‌سازمانی و کانال‌های گزارش‌دهی؛
  - شیوه‌های کاربردی گزارش دادن تخلف ازجمله پیرامون درخواست‌های شفاف‌سازی، درخواست اطلاعات بیشتر و ارائه بازخورد به افشاگر؛
  - سیاست محرمانگی و ناشناس ماندن شامل الزمات قانون محدودیت‌های اجرایی؛
  - ماهیت پیگیری به‌صورت‌های مختلف؛

- نوع محافظت و روش‌های پشتیبانی افشاگر از سوی سازمان؛ شامل شیوه‌ها و جبران اقدامات آسیب‌زا؛
- چگونگی پردازش اطلاعات شخصی و زمان صرف شده برای این کار.

- قوانین اجرایی شامل اینکه بر اساس مقررات ملی حفاظت از افشاگر، چه کسانی شامل این حفاظت می‌شوند و این مهم چگونه به انجام می‌رسد. همچنین تفاوت‌های احتمالی میان سیاست‌ها و شیوه‌های افشاگری و حفاظت از افشاگران درون‌سازمانی با قوانین موجود در این زمینه با این هدف که افراد بدانند در صورت افشاگری از چه حفاظت‌های قانونی برخوردار می‌شوند و تعهداتی که سازمان به شکل داوطلبانه برای سطح بالاتری از حفاظت تعریف کرده چیست؛
- اطلاعات تماس کانال‌های محرمانه و مستقل موجود برای مشاوره رایگان در بیرون از سازمان همچون مسئولان کشوری، اتحادیه‌های بازرگانی و سازمان‌های مدنی؛
- شیوه‌های گزارش‌دهی به بیرون و به مقامات مربوطه.

ارائه اطلاعات به کارکنان سازمان

- سازمان‌ها باید اطلاعات IWS را در اعلان‌های کتبی و الکترونیکی خود قرار دهند و برای انتشار آن‌ها از طیف گسترده‌ای از کانال‌ها و رسانه‌ها بهره گیرند. سازمان‌ها می‌توانند از بروشور، پوستر، بخش ویژه در وب‌سایت سازمان و مواردی از این دست استفاده کنند.
- سازمان‌ها وظیفه دارند به شکل پیوسته سیستم افشاگری درونی خود را تبلیغ کنند. این کار می‌تواند در نشست‌های پرسنلی با حضور همه پرسنل،

خبرنامه‌ها، نامه‌ها، ایمیل‌ها و کمپین‌های آگاهی‌رسانی همچون «هفته گفتن و شنیدن» انجام پذیرد.

- قراردادهای اشتغال باید همه کارکنان را ملزم به مطالعه و آگاهی از آیین‌نامه‌های سازمان در زمینه افشاگری و سیاست‌های حفاظت از افشاگر نمایند.
- سازمان‌ها باید برای همه مدیران و کارکنان، آموزش‌های آگاهی‌رسانی برگزار کرده و به‌صورت دوره‌ای اطلاعات مربوطه را برای آنان شرح دهند تا همه افشاگران احتمالی و افراد دخیل زیر پوشش قرار گیرند.

ارائه اطلاعات به دیگر افراد قادر به افشاگری و اشخاص دخیل

- سازمان‌ها باید اطلاعات مربوط به IWS را در وب‌سایت خود بگذارند، به‌نحوی‌که در یک بخش ویژه و به‌آسانی قابل دسترس باشد. هدف از این کار تضمین دسترسی همه افشاگران احتمالی و افراد دخیل به اطلاعات موردنیاز است.
- سازمان‌ها باید راه‌های ارتباطی مشخصی را برای طرف‌های بیرونی که ممکن است افشاگری کنند فراهم ساخته و در موارد موردنیاز این افشاگران بالقوه و افراد دخیل را در زمینه IWS آموزش دهند. کسانی مانند مشاوران، پیمانکاران، پیمانکاران فرعی، تأمین‌کنندگان و نیروهای آن‌ها در این حیطه قرار دارند.
- همه افشاگران احتمالی و افراد دخیلی که به‌نحوی با سازمان قرارداد دارند، باید طبق قرارداد ملزم به مطالعه و آگاهی از آیین‌نامه‌های سازمان در زمینه افشاگری و سیاست‌های حفاظت از افشاگر باشند. برای نمونه، این الزامات باید در قراردادهای مشاوران لحاظ گردد.

گسترش فرهنگ «گفتن و شنیدن»

نگاه افشاگران احتمالی (کارکنان و افراد مربوطه) به ارزش‌هایی که از سوی رؤسا و همکاران و ریاست سازمان بیان می‌گردد در تصمیم‌گیری آنان برای ابراز دغدغه‌هایشان در چارچوب IWS نقش دارد.

نگاه حمایتی «از بالا به پایین»

- ریاست سازمان (مدیرعامل، اعضای هیئت‌مدیره، رئیس سازمان و مدیران ارشد) باید پیوسته در زمینه IWS به‌عنوان یک اولویت سازمانی با کارکنان در ارتباط باشند و به شکل مستمر و حمایتی پیام‌رسانی کنند. این ارتباطات می‌تواند کتبی یا رودررو و درون‌سازمانی یا با طرف‌های دخیل بیرون از سازمان و حتی عموم مردم باشد.
- ریاست سازمان باید با رفتار و کنش خود از این ارتباطات پشتیبانی نموده و مشخصاً تعهد ریاست را نسبت به پاکدستی، حفاظت از افشاگران و رسیدگی به تخلفات صورت‌گرفته در سازمان نشان دهد.

مدیریت اخلاقی

- نگاه سازمان در زمینه افشاگری باید در سلسله‌مراتب مدیریتی از بالا به پایین منتقل شود. همه سطوح مدیریتی و سرپرستان باید پشتیبانی خود از IWS را ابراز نمایند.

سازمان‌ها باید در راستای پایبندی به فرهنگ «گفتن و شنیدن» و پیاده‌سازی IWS هر ساله برای عموم گزارش منتشر کنند.

- سازمان‌ها بایستی مدیران سلسه‌مراتبی را در قبال رسیدگی به گزارش‌های افشاگری پاسخ‌گو بدانند، به‌ویژه مدیرانی که در سیاست‌های تعریف‌شده سازمانی مسئول دریافت این گزارش‌ها هستند. بهتر است مسئولیت‌های مدیران در این زمینه به‌عنوان یکی از جنبه‌های ارزیابی کارکردشان تعریف گردد.

تشویق و قدردانی

- سازمان‌ها باید در قبال بیان اشکالات توسط افشاگران از آنان قدردانی کرده و در صورت رضایت‌شان این قدردانی را در سطح مدیران ارشد و عموم با ابزارهایی مانند جایزه محقق نمایند.

فرهنگ کلی اعتماد، شفافیت و پاسخ‌گویی

- سیستم‌های افشاگری درونی نمی‌توانند در انزوا کار کنند. آن‌ها بخشی از برنامه پاکدستی و قانون‌مندی سازمان هستند. ازاین‌رو رویکرد «گفتن و شنیدن» باید در فرهنگ سازمانی به پرورش اعتماد، شفافیت و پاسخ‌گویی کمک نماید.

پاسخ‌گویی به طرف‌ها در چارچوب شفافیت و گزارش‌دهی همگانی

- این گزارش‌دهی یکی از مؤلفه‌های اداره خوب، شفاف و پاسخ‌گو محسوب می‌شود و می‌تواند به اعتبار سازمان و پیاده نمودن سیستم افشاگری درونی کمک کند.
- گزارش‌های سالانه از کارکرد IWS و کارهای انجام‌شده در راستای پشتیبانی از فرهنگ «گفتن و شنیدن» در سازمان باید به هیئت‌مدیره، مدیران، کارکنان و دیگر طرفین دخیل مانند سهامداران ارائه گردد. این گزارش‌ها همچنین باید در وب‌سایت سازمان (برای نمونه در بخش IWS) منتشر گردیده و در

گزارش‌های مربوط به حوزه‌هایی همچون پاسخ‌گویی و اداره سازمان جای داده شود.

- گزارش‌دهی هر سازمان باید این موارد را پوشش دهد:
  - به‌کارگیری، خروجی‌ها و درس‌های آموخته‌شده از IWS شامل داده‌های انباشته و ناشناس پیرامون تعداد گزارش‌های دریافت‌شده، اقدامات واکنشی انجام‌شده و خروجی‌ها. این موارد می‌تواند دربردارنده زیان‌های مالی، غرامت‌ها، استردادها؛ زمان رسیدگی به پرونده‌ها و انواع تخلفات گزارش‌شده باشند. این داده‌ها برای نشان دادن رسیدگی مقتضی به گزارش‌های افشاگری ضروری هستند؛
  - حفاظت از افشاگران شامل ثبت تعداد شکایت‌ها از رفتارهای آسیب‌زا، اقدامات انجام‌شده برای پیگیری این موارد، خروجی‌های این موارد، زمان صرف‌شده برای حل‌وفصل پرونده‌ها و انواع تدابیر حفاظتی انجام گرفته برای افشاگران؛
  - آگاهی و اعتماد در بخش IWS؛ برای نمونه آنالیز نتایج بررسی‌ها.

سرمایه‌گذاران بالقوه، شرکا و کارکنان اغلب به IWS سازمان، آمارهای آن و میزان کارآمدی آن توجه دارند. انتشار اطلاعات فراگیر IWS سازمان به شیوه شفاف و در دسترس نشان می‌دهد که سازمان در گسترش فرهنگ افشاگری پیگیر است و آن را از بالاترین اولویت‌های استانداردهای اخلاقی خود می‌شمارد.

شیوه‌ها

بخشی از سیستم افشاگری درونی سازمان‌ها، راه‌اندازی سیستم‌هایی برای دریافت گزارش‌های افشاگری و پیگیری آن‌هاست. این امر شامل ایجاد کانال‌ها، شیوه‌ها و فرآیندهای گوناگون است.

بخشی از IWS، کانال‌های گوناگون افشاگری هستند که امن و دسترس‌پذیر بوده و امکان گزارش‌دهی کتبی و شفاهی را فراهم می‌سازند. سازمان‌ها باید مدیران سلسله‌مراتبی خود را به‌عنوان گیرنده‌های احتمالی گزارش‌های افشاگری در نظر بگیرند.

کانال‌های افشاگری گوناگون

- سازمان‌ها باید کانال‌های افشاگری درونی خود را به شیوه‌ای امن طراحی کنند. کارکرد این کانال‌ها باید به‌گونه‌ای باشد که هویت افشاگر و اشخاص ثالث مورد اشاره در گزارش‌های افشاگری پنهان بماند و پرسنل غیرمجاز امکان دسترسی به این گزارش‌ها را نداشته باشند.
- سازمان‌ها در هنگام راه‌اندازی کانال‌های افشاگری بایستی شرایط گوناگون افشاگران احتمالی را در نظر بگیرند و عواملی همچون موانع زبانی، جنسیت، سواد ناکافی، ناتوانی‌های فیزیکی، دسترسی به اینترنت و امکان ارائه گزارش در ساعات اداری و بیرون از آن را لحاظ نمایند.
- کانال‌های افشاگری ایجاد شده برای گزارش‌های کتبی باید دارای گزینه‌های آنلاین همچون ایمیل، وب و گزینه‌های آفلاین مانند پست فیزیکی و صندوق‌های دریافت گزارش باشند. کانال‌های افشاگری شفاهی نیز باید گزینه‌های از راه دور همچون تلفن و دیدار رودررو داشته باشند.
- دسته‌کم یک کانال افشاگری باید امکان گزارش‌دهی ناشناس داشته باشد.

- IWS باید کانال‌های ارتباطی امنی میان افشاگر و مسئول افشاگری فراهم آورد؛ به‌گونه‌ای که امکان ارسال مدارک پیوست در آن‌ها باشد. این ویژگی بایستی در کانال افشاگری ناشناس نیز لحاظ شود. برای نمونه می‌توان از پلتفرم‌های گزارش‌دهی آنلاین یا طرف‌های بیرونی استفاده کرد.

پلتفرم‌های گزارش‌دهی آنلاین

راه‌اندازی یک کانال افشاگری ناشناس و امن می‌تواند به‌لحاظ فنی پیچیده باشد. در این میان، سازمان‌ها مجبور نیستند این سیستم‌ها را از صفر بسازند بلکه می‌توانند از پلتفرم‌های افشاگری منبع – باز و یا ارائه‌دهندگان این پلتفرم‌ها استفاده نمایند.

در بخش پاسخ‌گویی U4 شفافیت بین‌الملل، مجموعه‌ای از رایج‌ترین سیستم‌های افشاگری مبتنی بر وب معرفی شده‌اند. این مطلب به ویژگی‌های مهم این سیستم‌ها یعنی ناشناسی، امنیت، دسترس‌پذیری و هزینه به‌صورت مزایا و معایب اشاره کرده است. در این مطلب همچنین مبانی اساسی و ملاحظات اجرایی سیستم‌های گزارش‌دهی شرح داده شده و مهم‌ترین تهدیدات دیجیتالی این تکنولوژی و راه‌کارهای برخورد با آن‌ها بیان گردیده است. در پایان این‌گونه نتیجه‌گیری‌شده که ابزارهای منبع – باز به‌لحاظ امنیت، برترین گزینه‌های موجود برای افشاگری هستند؛ درحالی‌که شرکت‌های ارائه‌دهنده چنین سرویس‌هایی بیشتر روی کارایی و کارکردهای مدیریت یکپارچه آن‌ها تمرکز نموده‌اند.

مدیران سلسله‌مراتبی

- سازمان‌ها باید مدیران سلسله‌مراتبی را دریافت‌کننده احتمالی گزارش‌های افشاگری درونی در نظر بگیرند، چراکه آن‌ها طبیعی‌ترین و پرکاربردترین کانال‌های گزارش مسائل کاری در زندگی روزمره هستند.
- در سیستم‌های افشاگری درونی باید به آموزش‌های لازم مدیران پرداخته شود. بااین‌وجود سازمان‌ها باید اعلام کنند که گزارش دادن به مدیران سلسله‌مراتبی ممکن است در سطح گزارش‌دهی به دایره افشاگری ـ از طریق کانال‌های تعریف‌شده ـ ضامن بی‌طرفی، پنهان ماندن هویت و کارایی فرآیند دریافت و رسیدگی نباشد.

کانال‌های گزارش‌دهی به‌واسطه سرویس‌دهندگان بیرونی

- اگر یک سازمان تصمیم بگیرد وظیفه اجرای کانال‌های گزارش‌دهی را به یک سرویس‌دهنده بیرونی بسپارد، این وظیفه به دریافت و تأیید گزارش‌ها، (در صورت درخواست سازمان) انجام تحقیقات موردبه‌مورد و دادن بازخورد آن به افشاگر محدود می‌شود. **در هر صورت مسئولیت پیگیری گزارش‌های، رسیدگی به تخلف شناسایی شده و ارائه بازخورد به افشاگر بردوش سازمان می‌باشد.**
- سازمان باید اطمینان حاصل کند که سرویس‌دهنده بیرونی (شرکت نرم‌افزاری ارائه‌دهنده خدمات وب‌سرویس) از مقتضیات قانونی و کارکرد مناسب IWS پیروی می‌کند. ازجمله اینکه هویت افشاگر و دیگر افراد دخیل را پنهان نگه می‌دارد و ارتباطات مناسبی با افشاگر برقرار می‌کند. ضمانت‌های لازم برای استقلال و محرمانگی باید در قرارداد با سرویس‌دهنده بازتاب پیدا کند و در صورت تخطی از تعهدات تعریف‌شده در این زمینه، مسئولیت‌های آن متوجه سرویس‌دهنده و سازمان می‌باشد.
- نقش، وظایف و مسئولیت‌های سرویس‌دهنده بیرونی باید به‌روشنی مشخص گردیده و به اطلاع افشاگران احتمالی رسانده شود.

کانال‌های اطلاعات و مشاوره

- هر سیستم افشاگری درونی می‌تواند دارای کانال‌های محرمانه‌ای باشد که افشاگران و دیگر طرف‌ها بتوانند اطلاعات فراگیر و راهنمایی‌های لازم را در زمینه دامنه شیوه‌های IWS از راه آن‌ها دریافت کرده و به جزئیات حفاظت در برابر رفتارهای آسیب‌زا، غرامت‌های تعیین‌شده و حقوق افراد دخیل دسترسی داشته باشند.
- سازمان‌ها باید درباره کانال‌های مشاوره مستقل؛ محرمانه و بدون‌هزینه در بیرون از سازمان به افشاگران احتمالی اطلاع‌رسانی کنند. این کانال‌ها معمولاً به‌وسیله مقامات کشوری، اتحادیه‌های بازرگانی و سازمان‌های مدنی اداره می‌شوند.
- کسانی که در جستجوی اطلاعات و مشاوره در زمینه افشاگری هستند، باید به‌طورکامل مورد محافظت قرار گیرند. این افراد باید در برابر نقض محرمانگی و رفتارهای آسیب‌زا مصون باشند.

IWS باید دقیق و کارآمد باشد. یعنی اجرای آن همراه با ریزبینی، زمان‌سنجی، عدالت و بی‌طرفی بوده و در آن تشخیص رخ دادن تخلف، رسیدگی به تخلفات تأییدشده و درست کردن مشکلات سیستماتیک شناسایی‌شده به‌کار بسته شوند. همچنین، پیگیری هر گزارش باید با مشارکت حقیقی افشاگر همراه باشد.

اقدام نمودن در قبال گزارش‌های افشاگری

- سازمان‌ها وظیفه دارند با طراحی و پیاده‌سازی فرایندها و شیوه‌هایی، اطمینان حاصل کنند که پیگیری گزارش‌های افشاگری به شکل دقیق، عادلانه، بی‌طرفانه و حساسیت زمانی صورت می‌گیرد. فرایند پیگیری باید در

چارچوب مراحل تعریف‌شده انجام گیرد و برای همه تصمیماتی که در پایان هر مرحله گرفته می‌شود معیارهای روشنی وجود داشته باشد.[1] مراحل تعریف‌شده پیگیری عبارت‌اند از: ارزیابی اولیه، تحقیقات و ترتیب اثر. IWS وظیفه دارد در صورت درخواست افشاگر یا افراد دخیل، برآوردی از عدالت و کیفیت پیگیری هر گزارش ارائه نماید.

- سازمان‌ها باید پیگیری گزارش‌های افشاگری و ارائه بازخورد به افشاگران را به چشم تعهد ببینند و اشتباهات احتمالی فرد مسئول پیگیری گزارش را در نظر گرفته و درصورتی‌که افراد مسئول در انجام وظایف خود دچار اشتباه شدند و سزاوار اقدام انظباطی بودند، سازمان باید بازخورد این مسئله را به افشاگر بدهد. گاه شرایطی به‌وجود می‌آید که این اشتباهات زمینه رفتار آسیب‌زا نسبت به افشاگر را ایجاد می‌کنند.[2]
- پیگیری گزارش‌ها باید با رعایت قوانین دقیق حفظ محرمانگی صورت گرفته و مبنای قرار دادن هرگونه اطلاعات در اختیار هر فرد، نیاز به آگاهی از آن باشد.

ارتباطات با افشاگران و مشارکت آنان

افشاگران به‌عنوان طرف‌های ذی‌نفع و آگاه بایستی در تمامی طول فرایند آگاه نگه داشته شده و فرصت‌های حقیقی برای ارائه دیدگاه‌های خود در روند رسیدگی به گزارش را داشته باشند.

---

۱. این قاعده همه گزارش‌های ناشناس را در برمی‌گیرد.

۲. در چنین مواردی، سازمان‌های بزرگ باید دارای سازوکارهایی برای شکایت باشند. این سازوکارها باید مستقل از افراد مسئول رسیدگی به گزارش بوده و اجرای آن برعهده کسانی باشد که از شایستگی لازم برای پیگیری گزارش‌های مربوط به اشتباهات رسیدگی برخوردار باشند و بازخورد لازم را به افشاگر بدهند.

- سازمان‌ها موظف‌اند دریافت هر گزارش افشاگری را در بازه زمانی دقیق و کوتاه اعلام نموده و به این موارد پایبند باشند:
  - امکان شفاف‌سازی گزارش و ارائه اطلاعات یا شواهد بیشتر توسط افشاگر؛
  - بازه‌ی زمانی که در آن با افشاگر تماس گرفته‌شده و در صورت نیاز از وی برای شفاف‌سازی یا ارائه اطلاعات بیشتر درخواست می‌شود؛
  - بازه‌های زمانی ارائه بازخورد پیگیری گزارش به افشاگر؛
  - مسئولیت‌های افشاگران ازقبیل محرمانه نگه داشتن هویت افراد دخیل در مسئله؛
  - IWS، مواردی مانند آگاهی‌بخشی در زمینه سیاست‌های افشاگری و حفاظت از افشاگران درون‌سازمانی را برعهده دارد.
- ارتباطات با افشاگر باید به‌صورت پیوسته و در تمام فرایند پیگیری انجام شود. افشاگر در هر زمان حق دارد:
  - درباره گزارش خود شفاف‌سازی کند و اطلاعات یا شواهد بیشتری ارائه نماید. وی در این زمینه تعهدی ندارد.
  - نگرانی‌های خود در ارتباط با ریسک‌های رفتار آسیب‌زا و پنهان نگه داشتن هویتش را ابزار نماید.
- ارتباط با افشاگر باید همراه با بازخوردهای مستمر و در زمان مناسب باشد. در این زمینه:
  - نخستین بازخورد، بایستی در بازه زمانی سه ماهه از دریافت گزارش داده شده و به پس از مرحله ارزیابی موکول نگردد.

- در حین فرایند پیگیری، بازخوردها باید در هر مرحله داده شده و فاصله‌های زمانی بین آن‌ها از سه ماه فراتر نرود.

- بازخوردهایی که به افشاگر داده می‌شود باید دارای این اطلاعات باشد:
  - اقدامات در نظر گرفته‌شده یا انجام‌شده در چارچوب پیگیری گزارش و زمینه‌های پیگیری و بازه زمانی پیش‌بینی‌شده.[1]
  - اقدامات انجام‌شده برای حفاظت از هویت افشاگر و ناشناس ماندن وی و همچنین حمایت‌های موجود و در صورت نیاز، اقدامات انجام‌شده برای حفاظت از افشاگر در برابر رفتارهای آسیب‌زا.
  - زمانی که افشاگر می‌تواند منتظر دریافت بازخورد بیشتر درباره پیگیری گزارش باشد.
- سازمان‌ها بایستی افشاگران را از یافته‌ها و نتایج پیگیری گزارش آگاه سازند. این آگاهی‌رسانی شامل اطلاعات به‌دست‌آمده از تحقیقات پیرامون اتهامات وارده، (در صورت وجود) به انجام نرسیدن تحقیق روی برخی اتهامات و دلیل آن و همچنین محدودیت‌های مهم در انجام تحقیقات می‌باشد.[2] افزون‌براین، نتایج به‌دست‌آمده از بررسی هر اتهام (وارد بودن، وارد نبودن، نامشخص بودن) و نمای کلی اقدامات اصلاحی در شرایط مقتضی باید به آگاهی افشاگر رسانده شود. افشاگر باید فرصت بررسی و ارائه دیدگاه‌های

---

۱. در مواردی که سازمان به دلایلی همچون محدودیت اطلاعات تنها می‌تواند بازخوردهای محدودی به افشاگر بدهد، باید این مسئله را به‌روشنی به افشاگر توضیح دهد. برای نمونه به وی توضیح دهند که سازمان به‌دلیل تعهد خود به محرمانه نگه داشتن اطلاعات دیگر پرسنل یا محدودیت‌های قانونی نمی‌تواند بازخورد کاملی به افشاگر بدهد.

۲. برای نمونه ممکن است برای مصاحبه با برخی از افراد و گرفتن اظهارنامه و مطابقت دادن حقایق پیدا شده، محدویت‌هایی وجود داشته باشد. رایج‌ترین دلایل این محدودیت‌ها رفتن افراد موردنظر از سازمان، خارج شدن این افراد از کشور و خودداری آن‌ها از همکاری می‌باشد.

خود درباره این نتایج را پیدا کند و نقطه‌نظرات وی در گزارش پیگیری درج گردد.

ارزیابی اولیه گزارش‌های افشاگری

- همه گزارش‌های افشاگری دریافت‌شده بایستی ثبت گردیده، دریافت‌شان تأیید شده و با ریزبینی ارزیابی شوند.
- در صورت نیاز، فرد پیگیری‌کننده گزارش باید از افشاگر درخواست اطلاعات بیشتر کند.
- پس از گرفتن گزارش و در حین فرایند پیگیری آن، فرد مسئول باید پیوسته ریسک رفتار آسیب‌زا در قبال افشاگر را ارزیابی نماید. سازمان وظیفه دارد برای پیشگیری از رفتار آسیب‌زا به توصیه مسئول افشاگری تدابیر لازم را به انجام برساند.
- فرد مسئول پیگیری گزارش پس از دریافت آن و در حین فرایند پیگیری باید پیوسته ریسک رفتار آسیب‌زا در قبال همه افراد دخیل، سازمان و منافع عمومی را ارزیابی نماید. سازمان وظیفه دارد در راستای حفاظت و پشتیبانی از این طرف‌ها، به توصیه مسئول افشاگری تدابیر لازم را انجام دهد.
- در سازمان‌هایی که شمار زیادی از گزارش‌های افشاگری دریافت می‌شود، لازم است پیگیری این گزارش‌ها بر مبنای ریسک اولویت‌بندی شود. این ریسک شامل ریسک آسیب به فرد، منافع عمومی و سازمان می‌شود. درعین‌حال، رسیدگی به همه گزارش‌ها با توجه به حساسیت زمانی باید تضمین گردد.

- درصورتی‌که مشخص شود یک گزارش فراتر از دامنه IWS است، می‌توان افشاگر را به دیگر سیستم‌های گزارش‌دهی یا ثبت شکایت درون‌سازمانی راهنمایی کرد. اگر گزارش دریافت‌شده از کانال‌های افشاگری درونی دامنه پیچیده یا مبهم داشته باشد، رسیدگی به آن باید در IWS و در صورت نیاز در هماهنگی با دیگر سیستم‌های گزارش‌دهی درون‌سازمانی انجام شود.

تحقیقات درباره تخلفات گزارش‌شده

- کسانی که به گزارش‌ها رسیدگی می‌کنند از افشاگر، افراد دخیل و دیگر طرف‌های مربوطه استقلال کافی داشته و توانایی انجام تحقیقات فرامرزی را دارا باشند.
- تحقیقات باید برمبنای یک فرایند مشخص پیگیری شود. فردی که گمان تخلف وی می‌رود تا مشخص شدن نتایج تحقیقات باید بی‌گناه محسوب شده و از حق پاسخ‌گویی و کمک گرفتن برخوردار باشد. درعین‌حال مسئول تحقیق حق ندارد اطلاعاتی را که ممکن است به آشکار شدن هویت افشاگر منجر شود در اختیار متهم قرار دهد.
- فرد مسئول تحقیق باید مراجع، دامنه، روش‌ها و مهارت‌های تحقیقات را به‌طور شفاف مشخص نماید. تحقیقات باید از منابع مناسب برخوردار بوده و کسانی که آن‌ها را انجام می‌دهند چه در درون سازمان و چه بیرون از آن، بایستی شایستگی‌های لازم را دارا باشند.
- در پرونده‌هایی که با مواردی مانند زورگویی، آزار جنسی، اخاذی جنسی یا بهره‌برداری جنسی همراه‌اند، تحقیقات باید با رعایت اصول «تمرکز بر قربانی/بازمانده» انجام گیرد. در این شرایط باید از هر اقدامی که آسیب روانی را برای

افراد تکرار می‌کند پرهیز شود و سلامت، نیازها و خواسته‌های قربانیان در اولویت قرار داده شود.

- سازمان‌ها وظیفه دارند پروتکل‌های تحقیقاتی را مدنظر قرار دهند.
- نتایج تحقیقات تا زمانی که به اطلاع افشاگر رسیده و پس از ارزیابی وی، دیدگاه‌هایش در گزارش تحقیق درج شود، نبایستی قطعی تلقی گردند.

ترتیب اثر

- یک پرونده هنگامی بسته می‌شود که به نتیجه رسیده باشد و هیچ اطلاعات دیگری که خروجی پرونده را تغییر دهد در اختیار نباشد. در صورت نیاز، مانند مواردی که افشاگر ادعاهای مستند یا شواهد تازه‌ای می‌آورد، پرونده باید دوباره باز شود و تحقیقات به جریان افتد.
- اگر تحقیقات به این نتیجه بینجامد که تخلفی رخ داده، در حال رخ دادن است یا احتمالاً رخ خواهد داد، آنگاه سازمان‌ها موظف‌اند اقدامات لازم را جهت رسیدگی انجام دهند. این اقدامات بسته به اقتضاء عبارت‌اند از:
  - جلوگیری یا پیشگیری از تخلف؛
  - مجازات مسبّبان تخلف؛
  - جبران آسیب‌های وارده؛
  - دادن گزارش به مقامات مربوطه.
- صرف‌نظر از به اثبات رسیدن تخلف، سازمان‌ها باید تلاش لازم را برای شناسایی هرگونه اشکال سیستماتیک همچون ضعف در سیاست‌ها یا شیوه‌ها انجام دهند. هدف آن است که از بروز تخلف یا تکرار آن در آینده و ایجاد آسیب‌های جدی جلوگیری شود.

- سازمان‌ها باید تدابیر لازم برای حفاظت از افشاگران را به انجام رسانده و هویت آنان را پس از پایان پرونده پنهان نگه دارند.

ثبت و نگهداری از داده

گزارش‌های دریافت‌شده، اقدامات انجام‌شده برای پیگیری، یافته‌ها و خروجی پیگیری و همچنین ارتباطات با افشاگر و افراد دخیل باید مستند گردیده و با حفظ محرمانگی و مقتضیات حفاظت از داده به‌صورت قابل‌بازیابی و قابل‌بازرسی بایگانی شوند.

- سازمان‌ها وظیفه دارند با رعایت مقتضیات محرمانگی، تمامی گزارش‌های دریافتی را بایگانی نمایند. نگهداری از این گزارش‌ها پس از زمان مقتضی ضرورت نداشته و باید بر اساس الزامات قانونی باشد که همان پیگیری دقیق گزارش‌های افشاگری و حفاظت از افشاگر در برابر رفتار آسیب‌زا است.
- سازمان‌ها باید برای ثبت شمار گزارش‌های افشاگری دریافت‌شده، اقدامات انجام‌شده در قبال این گزارش‌ها و نتایج به‌دست‌آمده سیستم‌هایی برای بایگانی داشته باشند. اطلاعاتی همچون برآورد آسیب مالی وارده، غرامت، بازیابی (میزان بازگشت غرامت) و جریمه‌ها باید در محتوای این بایگانی‌ها درج شود. افزون‌براین، مواردی ازقبیل زمان رسیدگی به گزارش‌ها، نوع تخلفات گزارش‌شده، داده‌های بعدی ارائه‌شده به هیئت‌مدیره، پرسنل یا طرف‌های دیگر (مانند سهامداران و عموم) به‌صورت انباشته و ناشناس باید ثبت و نگهداری شوند.

اساس اجرای IWS با پردازش داده‌های شخصی همراه است. این داده‌ها مربوط به افشاگر، افراد دخیل و شاهدان هستند.

- طراحی و راه‌اندازی IWS سازمان بایستی با مشاوره مسئول درونی حفاظت از

داده انجام پذیرد. اگر چنین مسئولی در سازمان نباشد، این مشورت با مقامات فعال در زمینه حفاظت از داده در کشور انجام می‌شود.

- سازمان‌ها موظف‌اند با ارائه اطلاعات لازم به افشاگران احتمالی، آن‌ها را آگاه سازند که داده‌هایشان چگونه پردازش خواهد شد و چه مدت‌زمانی و با چه هدفی نگهداری می‌گردد.
- داده‌های شخصی که ارتباطی با رسیدگی به گزارش داده شده ندارد و نباید گردآوری شوند و در صورت گردآوری باید بی‌درنگ پاک شوند.

بایگانی گزارش‌های شفاهی برمبنای آیین‌نامه‌های اتحادیه اروپا

سازمان‌ها وظیفه دارند با رضایت افشاگر، گزارش‌های شفاهی مستندشده را به شکل کامل و دقیق بایگانی کنند. این بایگانی‌ها باید دوام‌دار و قابل بازیابی باشند.

- سازمان‌ها می‌توانند گزارش‌های شفاهی موجود در قالب ضبط گفتگوهای خط تلفن یا هرگونه سیستم ضبط پیام صوتی را مستند نمایند. آن‌ها می‌توانند گفتگوها را ضبط و بایگانی کرده و یا رونوشت دقیق و کامل آن‌ها را بایگانی نمایند. رونوشت باید به‌وسیله فرد مسئول رسیدگی به گزارش تهیه شود.
- درصورتی‌که گزارش‌ها شفاهی ارائه‌شده با خط تلفن ضبط نشود، سازمان‌ها می‌توانند تعداد دقیقه‌های گفتگو را توسط مسئول رسیدگی به گزارش ثبت کنند.
- سازمان‌ها می‌توانند گزارش‌های رودررو را به‌وسیله ضبط صدای گفتگو یا ثبت تعداد دقیقه‌های گفتگو مستند نمایند. این کار بایستی توسط مسئول رسیدگی به گزارش انجام شود.
- در ارتباط با تمامی گزارش‌های شفاهی، سازمان‌ها وظیفه دارند فرصت چک کردن، اصلاح و تأیید (با امضاء) مستندات تهیه‌شده با رونوشت یا ثبت دقیقه‌های گفتگو (یا دیدار) را در اختیار افشاگر بگذارند.

IWS و مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR)

سازمان‌هایی که در حوزه اتحادیه اروپا هستند بایستی ضامن رعایت الزامات فنی و سازمانی در سیستم افشاگری درونی خود باشند. این الزامات عبارت‌اند از:

- سازمان‌ها باید اهداف IWS را به روشنی مشخص نمایند.
- سازمان‌ها باید بتوانند ارزیابی و کاهش ریسک حریم خصوصی را در مراحل طراحی و پیاده‌سازی IWS نشان دهند. همچنین برخی سازمان‌های فعال در شماری از کشورها موظف‌اند گزارش‌های ارزیابی اثرات حفاظت از داده خود را به مقامات مربوطه در زمینه حفاظت از داده ارائه دهند.
- IWS باید با اصل کمترین داده کار کند و اطلاعات شخصی افراد تنها در صورت ضرورت و ارتباط با پرونده‌های در حال رسیدگی گردآوری شوند.
- IWS هر سازمان باید برای نگهداری از اطلاعات پردازش‌شده در جریان رسیدگی به پرونده‌های افشاگری، بازه‌های زمانی مقتضی تعریف کند. مبنای تعیین این بازه‌های زمانی، خروجی پیگیری پرونده‌ها است. برای نمونه در مورد گزارش‌هایی که در پایان مرحله ارزیابی اولیه مشخص گردد، دامنه آن‌ها فراتر از IWS است، این دست اطلاعات نباید در زمان تحقیقات نگهداری شوند.
- افراد درگیر در گزارش افشاگری شامل افشاگر، اشخاص دخیل و اشخاص ثالث مذکور در گزارش باید از نحوه پردازش اطلاعات شخصی‌شان آگاهی پیدا کنند. این آگاهی‌رسانی باید در اولین فرصت ممکن انجام گیرد. در پرونده‌هایی که آگاه کردن افراد درگیر در مرحله مقدماتی پیگیری ممکن است تحقیقات درباره گزارش را به خطر اندازد، می‌توان قرار دادن برخی اطلاعات در اختیار افراد دیگر را به تأخیر انداخت. تصمیم‌گیری درباره به‌تأخیرانداختن آگاهی‌رسانی بایستی به‌صورت موردی انجام شده و دلایل آن مستند گردد.
- درصورتی‌که یک سازمان بخشی از فرایند پیگیری گزارش‌های افشاگری (مانند کانال‌های افشاگری یا تحقیقات) را برون‌سپاری کند، موظف است قراردادی پیرامون پردازش داده‌های شخصی منعقد نماید.

منبع: سرپرست حفاظت از داده اروپا (۲۰۱۶)، «اصول پردازش اطلاعات شخصی در جریان رسیدگی به افشاگری».

محافظت و پشتیبانی از افشاگران

تضمین حفاظت کارآمد از افشاگران و دیگر طرف‌هایی که در معرض ریسک هستند نیازمند تدابیر گوناگون است؛ ازجمله حفاظت از هویت آن‌ها، جلوگیری، پیشگیری و رسیدگی به رفتارهای آسیب‌زا در قبال آنان و پشتیبانی از این افراد.

حفظ هویت افشاگران و اشخاص دخیل

سازمان‌ها در هنگام راه‌اندازی IWS باید چگونگی محافظت و پشتیبانی از تمامی گروه‌های بالقوه افشاگری و طرف‌های دخیل را مدنظر قرار دهند. این پوشش شامل افرادی است که امکان گزارش‌دهی از کانال‌های افشاگری درونی سازمان را دارا هستند و همچنین افرادی که قانون، حفاظت از آنان را ایجاب می‌کند. این دو گروه همواره یکسان نمی‌باشند.[1]

هویت و اطلاعات هویتی افشاگر (اطلاعاتی که بتوان به‌طور مستقیم یا غیرمستقیم هویت را از آن‌ها نتیجه‌گیری کرد) بدون رضایت صریح وی نباید آشکار شده و باید تنها در اختیار افراد صلاحیت‌داری که مسئول دریافت و پیگیری گزارش هستند، قرار گیرد.

محرمانگی

- سازمان‌ها موظف‌اند راه‌اندازی و اجرای IWS خود را به‌گونه‌ای انجام دهند که ضامن محرمانگی هویت افشاگر و طرف‌های مذکور در گزارش باشد. همچنین افراد غیرمجاز نباید امکان دسترسی به این اطلاعات را پیدا کنند.

---

۱. برای نمونه بیشتر قوانین حفاظت از افشاگر، افشاگران «بیرونی»، کاربران، مشتریان و بهره‌برداران را پوشش نمی‌دهند. این درحالی است که برخی سازمان‌ها امکان گزارش‌دهی با IWS را برای این گروه‌ها فراهم می‌کنند. درمقابل، بیشتر مقررات مانند اصول اتحادیه اروپا تنها سازمان‌ها را موظف نموده که امکان گزارش‌دهی از IWS را برای کارکنان خودشان فراهم سازند و درعین‌حال کسی که اطلاعات به‌دست‌آمده در ارتباط با فعالیت‌های کاری را گزارش می‌کند، زیر این پوشش حفاظتی قرار داده است.

- تمامی پرسنلی که صلاحیت دریافت یا پیگیری گزارش‌های افشاگری را دارند باید مقیّد به حفظ اصول محرمانگی باشند.
- تنها زمانی مجوز افشای هویت افشاگر وجود دارد که لزوم قانونی برای آن وجود داشته باشد. سازمان‌ها باید به‌وسیله کانال‌هایی مانند اعلام سیاست‌ها و آموزش، اطلاعات مربوط به موارد استثنای محرمانگی را در اختیار افشاگران احتمالی گذاشته و اگر آن‌ها اقدام به افشاگری کردند، در این زمینه با آن‌ها ارتباط برقرار کنند.
- در مواردی که سازمان تشخیص دهد برخی اطلاعات آشکار شوند، موظف است با اعلام مناسب و به‌صورت توضیح کتبی، افشاگر را از این مسئله آگاه نموده و تدابیر حفاظتی لازم را برای وی انجام دهد. افشاگر باید فرصت داشته باشد تا به تصمیم افشای هویتش اعتراض کند.
- IWS باید به روشنی برای افشاگران احتمالی توضیح دهد که حفاظت از آن‌ها در مورد محرمانه نگه داشتن هویتشان در عمل مسئله‌ای مطلق نیست. برای نمونه اگر سازمان بسیار کوچک باشد یا افشاگر پیش از ارائه گزارش، دغدغه‌های خود را با همکارانش مطرح کرده باشد، این خطر وجود دارد که کسانی به این نتیجه برسند که گزارش توسط وی داده شده است.
- سازمان‌ها وظیفه دارند مجازات‌های کارآمد، متناسب و بازدارنده‌ای برای تخلف در وظیفه محرمانه نگه داشتن هویت افشاگران تعیین نمایند.

سازمان‌ها وظیفه دارند گزارش‌های ناشناس را پذیرفته، پیگیری نموده و از افشاگران ناشناس حفاظت نمایند.

ناشناس ماندن

- دست‌کم یک کانال افشاگری درونی باید از قابلیت گزارش‌دهی ناشناس برخوردار باشد.
- باید یک کانال ارتباطی امن میان افشاگر و کسانی که مسئول پیگیری گزارش هستند وجود داشته باشد. برای نمونه سازمان‌ها می‌توانند از پلتفرم‌های گزارش‌دهی آنلاین یا طرف‌های بیرونی استفاده کنند.
- IWS باید به افشاگران احتمالی توضیح دهد که حفاظت ارائه‌شده در زمینه پنهان نگه داشتن هویت امری مطلق نیست. همچنین مشکلات اجرایی موجود در این زمینه باید برای آن‌ها بیان گردد؛ از جمله:
  - اگر سازمان بسیار کوچک باشد یا افشاگر پیش از ارائه گزارش دغدغه‌های خود را با همکارانش مطرح کرده باشد، این خطر وجود دارد که کسانی به این نتیجه برسند که گزارش توسط وی داده شده است.
  - ناشناس بودن به‌منزله آن است که فرد مسئول پیگیری گزارش نمی‌داند از چه کسی حفاظت می‌کند. این محدودیت ممکن است پیشگیری از آشکار شدن هویت افراد را برای فرد مسئول دشوار سازد.
- سازمان‌ها صرف‌نظر از اینکه خودکار دریافت و پیگیری گزارش‌های ناشناس را انجام می‌دهند یا خیر وظیفه دارند از تمامی کسانی که چه از کانال درونی و چه از کانال بیرونی اطلاعاتی درباره تخلف احتمالی ارائه می‌کنند و سپس شناسایی می‌شوند، حفاظت لازم را به‌عمل آورند.

مزایای پذیرش و پیگیری گزارش‌های ناشناس

- پذیرش گزارش‌های ناشناس به چند صورت به اعتمادسازی در IWS کمک می‌کند؛ از جمله:
  - به افشاگران و طرف‌های دخیل احتمالی نشان می‌دهد که برای سازمان رسیدگی به تخلفات مهم‌تر از پیدا کردن هویت فردی است که تخلف را افشا نموده است.
  - افراد را تشویق می‌کند دغدغه‌های خود را ابراز کنند، به‌ویژه کسانی که به‌خاطر ترس از پیامدهای منفی یا ترس از عدم تلاش کافی سازمان مربوطه برای حفاظت از هویتشان، اقدام به افشای مفاسد نمی‌کنند.
- گزارش‌های ناشناس می‌توانند اطلاعات ارزشمندی را درباره تخلفاتی که منافع عمومی را به خطر می‌اندازند در اختیار سازمان‌ها بگذارند.
  - به‌طورکلی نرخ اثبات گزارش‌های ناشناس از گزارش‌های افشاگری که فرد هویت خود را اعلام می‌کند، پایین‌تر است ولی فاصله زیادی با آن ندارد. می‌توان با بهره‌گیری از کانال‌های ارتباطی که امکان تبادل اطلاعات میان افشاگران ناشناس و مسئولان رسیدگی را ایجاد می‌کنند، این نرخ را بهبود بخشید.
  - گزارش‌های جزئی یا نادرست، شمار زیادی از کل گزارش‌ها را تشکیل می‌دهند، به‌ویژه در سازمان‌هایی که امکان گزارش‌دهی ناشناس وجود دارد.
- در عمل، افشاگران ناشناس معمولاً پس از تبادل اطلاعات اولیه با افراد مسئول پیگیری گزارش، هویت خود را آشکار می‌کنند.

حفاظت در برابر مداخله و رفتار آسیب‌زا

رفتار آسیب‌زا عبارت است از هرگونه تهدید یا بیان یا اقدام مستقیم یا غیرمستقیم چه در قالب فعل و یا ترک‌فعل که منجر به آسیب یا امکان آسیب به فردی که افشاگری کرده یا گمان افشاگری وی می‌رود باشد؛ ازجمله آسیب فیزیکی یا روانی، لطمه به آبرو، زیان مالی و ایجاد درد و رنج روحی و روانی. رفتارهای آسیب‌زا می‌توانند عمدی یا در نتیجه ناتوانی سازمان در پشتیبانی و حفاظت از افشاگر باشند. نمونه‌های رفتار آسیب‌زا:

- تعلیق، اخراج یا اقدامات همتای آن
- عدم تبدیل قرارداد کار موقت به قرارداد کار دائم
- عدم تجدید یا ابطال زودهنگام قرارداد کار موقت
- زمینه‌سازی برای استعفا (هنگامی که سازمان با ناگوار کردن شرایط، فرد را به‌سوی استعفا می‌برد).
- پایین آوردن رتبه کاری یا تعلیق ترفیع رتبه
- جابجا نمودن وظایف کاری، کاهش یا محدود ساختن مأموریت‌های کاری، تغییر در ساعات کار
- گزینش ناعادلانه برای انجام وظایف یا شرکت در رویدادها، تعلیق دوره‌های آموزشی
- حذف منابع در دسترس یا ایجاد محدودیت در آن همچون بودجه و منابع انسانی
- کاهش دستمزد یا تعلیق پرداخت
- ارزیابی منفی از کارکرد یا توصیه‌نامه‌های شغلی
- بازرسی یا تحقیقات بدون مجوز از کارکرد فرد در انجام وظایف، افشای نتایج بازرسی‌ها
- اعمال یا دستور انجام هرگونه اقدام انظباطی شامل توبیخ یا تنبیه
- رفتار قهرآمیز، ترساندن، آزار یا طرد کردن
- تبعیض، سرزنش یا رفتار ناروا
- بایکوت یا قرار دادن در لیست سیاه
- ابطال یا پایان دادن زودهنگام قراردادهای کالا و خدمات
- آشکار کردن هویت افشاگر
- پیگرد یا اقدام قانونی
- خشونت فیزیکی یا روانی
- آبروریزی، لطمه به اعتبار یا تحقیر فرد به‌وسیله پرس‌وجو از سلامت روان، شایستگی حرفه‌ای، اطمینان‌پذیری یا پاکدستی

جلوگیری از مداخله و رفتار آسیب‌زا

- سازمان‌ها باید تعریف گسترده‌ای از رفتار آسیب‌زا داشته باشند؛ به‌گونه‌ای که فعل و یا ترک‌فعل، منجر به آسیب افشاگر یا دیگر طرف‌های حفاظت شده نگردد. لیست رفتارهای آسیب‌زا در هر سازمان باید بدون کلی‌نگری بوده و حاوی مصداق‌هایی باشد که همه شکل‌های رفتار آسیب‌زا نسبت به افشاگرانی که پرسنل سازمان نمی‌باشند را تعریف کند. ازجمله مواردی که در سندهای سازمانی باید رفتار آسیب‌زا تلقی شود می‌توان به گذاشتن افراد در لیست سیاه، پایان دادن زودهنگام قراردادهای تأمین کالا و خدمات و همچنین لغو گواهی یا مجوز اشاره کرد.

سازمان‌ها باید از هرگونه رفتار آسیب‌زا در ارتباط با افشاگر و هرگونه مداخله در افشاگری جلوگیری نمایند.

آیین‌نامه‌های رفتاری و اخلاقی و سیاست‌های سازمان در زمینه ممانعت از رفتارهای ناشایست با افشاگران باید شامل موارد زیر باشند:

- رفتار آسیب‌زا به هر شکل در قبال افشاگران و اشخاص ثالث مورد محافظت؛ ازقبیل تهدید به اقدام آسیب‌زننده و تلاش در جهت انجام آن شامل جستجوی هویت افشاگر؛
- ایجاد مانع یا تلاش برای ایجاد مانع بر سر راه افشاگری (مداخله در افشاگری)؛
- سازمان‌ها بایستی برای رفتارهای آسیب‌زا در قبال افشاگر و مداخله در کار افشاگری مجازات‌هایی در نظر بگیرند.

پیشگیری از رفتار آسیب‌زا

سازمان‌ها وظیفه دارند در راستای پیشگیری از رفتار آسیب‌زا و تضمین مصون ماندن افراد و نهادهای زیرشاخه یا در کنترل خود از رفتار آسیب‌زا، تدابیر مناسب و منطقی بیندیشند.

سازمان‌ها باید به صراحت پایبندی خود به خودداری از ورود به قراردادهایی که حقوق و حفاظت از افشاگران را نقض یا مخدوش می‌کند، اعلام نمایند. ازجمله این قراردادها می‌توان به معاهدات حل‌وفصل پیش‌تعارضی، مواد قراردادی وفاداری و بندهای تعهدی محرمانگی و عدم افشاء اشاره نمود. به‌این‌منظور، بهتر است رویکرد سازمان نسبت به چنین قراردادها و تعهداتی به صراحت در اسنادی که در زمینه حقوق و حفاظت از افشاگر در IWS تعریف می‌شود، تدوین شود و آشکارا ثبت گردد که در صورت بروز تعارض اصول و قواعد سازمانی با سیاست‌های افشاگری، این سیاست‌ها چیره خواهد بود و ملاک قرار می‌گیرند.

- هر سازمان باید اطمینان حاصل نماید که همه افراد و نهادهای زیرمجموعه مستقیم و غیرمستقیم یا دارای قرارداد، از ممنوعیت رفتارهای آسیب‌زا نسبت به افشاگران در آیین‌نامه‌های رفتاری و سیاست‌های افشاگری آگاه هستند و می‌دانند که سازمان این رفتارها را مجازات خواهد کرد. طرف‌هایی که باید از این مسائل آگاه باشند عبارت‌اند از: کارکنان و نهادهای کنونی و پیشین سازمان، پرسنل اجرایی، اعضای هیئت‌مدیره، کارآموزان، دانشجویان شاغل، داوطلبان، پیمانکاران، زیرمجموعه‌های پیمانکاران، تأمین‌کنندگان و مشاوران.
- سازمان‌ها موظف‌اند با اجرای استراتژی‌های مناسب همچون برآورد ریسک پیوسته و سیستماتیک و تدابیر پیش‌گیرانه، در طول فرایند پیگیری گزارش‌ها و پس از بسته شدن پرونده‌ها از بروز هرگونه رفتار آسیب‌زا در قبال افشاگران

پیشگیری نمایند.

- به‌منظور پیشگیری از ریسک آسیب بیشتر به افشاگر، سازمان‌ها وظیفه دارند در هنگام رسیدگی به شکایت‌های درونی رفتار آسیب‌زا، اقدامات لازم مانند تعلیق فرایندهای انضباطی و دادن مرخصی با دستمزد را به انجام رسانند.[1]
- ناتوانی فرد مسئول انجام اقدامات لازم برای پیشگیری از رفتار آسیب‌زا، بایستی ناتوانی در انجام وظیفه تلقی شده و در این چارچوب رسیدگی شود. در برخی موارد این ناتوانی‌ها به رفتار آسیب‌زا نسبت به افشاگر منجر می‌شود[2].

رسیدگی به رفتار آسیب‌زا، مداخله و نقض محرمانگی

IWS باید دارای سازوکارهای قابل اجرا، شفاف و بهنگام باشد تا (۱) شکایت‌ها از رفتارهای آسیب‌زا، مداخلات و نقض محرمانگی را دریافت و پیگیری کند، (۲) افراد خطاکار را مجازات نماید و (۳) جبران کامل خسارت‌های افشاگران و دیگر طرف‌های حفاظت‌شده را تضمین نموده و تدابیر لازم برای جبران و دادن غرامت به آنان را انجام دهد.

سازمان‌ها باید از سازوکارهای قابل اجرا، شفاف و بهنگامی برای دریافت و پیگیری شکایت‌ها پیرامون موارد زیر برخوردار باشند:[3]

- رفتار آسیب‌زا در قبال افشاگر و طرف‌های سوم حفاظت شده؛
- مانع‌تراشی یا تلاش برای انجام آن در کار افشاگری (مداخله)؛
- نقض محرمانگی هویت افشاگر.

---

۱. این قانون زمانی باید اجرا شود که مشخص گردد فردی که از رفتار آسیب‌زا شکایت کرده، پیش‌تر اطلاعاتی را به‌صورت درونی یا بیرونی گزارش نموده یا برای دیگران افشاء کرده و سپس با رفتار آسیب‌زا روبه‌رو شده است.

۲. در سازمان‌های بزرگ باید یک سازوکار شکایت مستقل از افراد مسئول پیگیری گزارش‌ها وجود داشته باشد که از شرایط لازم برای دریافت و پیگیری گزارش‌های ناتوانی در رسیدگی برخوردار بوده و بازخورد لازم را به افشاگر بدهد.

۳. به‌منظور پنهان نگه داشتن هویت افشاگر، این سازوکارها باید بخشی از IWS باشند نه سیستم‌های رسیدگی به شکایات و حل‌وفصل اختلافات.

- اگر انجام رفتار آسیب‌زا تأیید گردد، سازمان باید با انجام تدابیر لازم تضمین کند که:
  - رفتار آسیب‌زا متوقف می‌شود؛
  - کسی که دچار رفتار آسیب‌زا گردیده، مورد محافظت فیزیکی، مالی و روانی قرار می‌گیرد؛
  - خسارت‌ها به بهترین شکل ممکن جبران شوند. ازجمله زیان‌های آتی غیرمستقیم و زیان‌های مالی و غیرمالی و علاوه بر این، افشاگر به جایگاهی که پیش از رفتار آسیب‌زا در آن بوده بازگردانده می‌شود.

نمونه‌های اقدامات جبرانی

- بازگرداندن فرد به جایگاهی که پیش از رفتار آسیب‌زا در آن بوده و یا جایگاهی مشابه با دستمزد، شرایط و شرح وظایف یکسان.
- دسترسی عادلانه به هرگونه ترفیع یا آموزشی که معلق شده بود.
- بازگردادن وظایت در صورت امکان.
- جبران زمان ازدست‌رفته و تأثیر به‌وجودآمده روی کارکرد فرد.
- لغو پیگرد قانونی افشاگر.
- از بین بردن همه اسنادی که حاوی اطلاعاتی در زمینه قرارگیری در لیست سیاه یا تلافی است.
- به جریان انداختن دوباره هرگونه فرایند تهیه وسایل.
- پوزش خواستن به‌دلیل ناتوانی.
- برقرار نمودن هرگونه قرارداد لغو شده.
- تشویق به‌خاطر پایبندی به روند، ارزش‌ها و منافع سازمان به شیوه برملا نمودن تخلفات؛ برای نمونه دادن جایزه افشاگری.
- جبران زیان‌های مالی ناشی از درآمدهای گذشته، حال و آینده.
- جبران زیان‌های مالی ناشی از درد، رنج و هزینه‌های درمانی.

بازخواست از مسئولان رفتار آسیب‌زا، مداخله و نقض محرمانگی

- سازمان‌ها وظیفه دارند در برخورد با موارد زیر مجازات‌های کارآمد، متناسب و بازدارنده‌ای در نظر بگیرند:
  - رفتار آسیب‌زا در قبال افشاگر و طرف‌های سوم حفاظت‌شده؛
  - مانع‌تراشی یا تلاش برای مانع‌تراشی بر سر راه افشاگری (مداخله)؛
  - نقش محرمانگی هویت افشاگر.
- رفتار آسیب‌زا، مداخله یا نقض محرمانگی هویت افشاگر توسط کارکنان سازمان بایستی یک تخلف جدی و فاحش تلقی گردد. در صورت بروز چنین تخلفاتی، لازم است یک فرایند رسمی رسیدگی انضباطی برای خطاکاران به جریان افتد.
- سازمان‌ها باید رویکردها و مجازات‌های مناسبی در قبال بروز رفتار آسیب‌زا از سوی کسانی مانند مشاوران، تأمین‌کنندگان، اعضای هیئت‌مدیره و داوطلبانی که پرسنل‌شان نیستند و شامل رویکردهای انضباطی نمی‌شوند، تعریف نمایند. برای نمونه سازمان‌ها می‌توانند آن‌ها را از جایگاهی که هستند بردارند و به قرارداد خود با آن‌ها پایان دهند. بروز چنین وضعیت‌هایی باید در مفاد قراردادهای سازمانی با طرف‌های بیرونی پیش‌بینی شود.
- در مواردی که رفتار آسیب‌زا با نقض قانون همراه است، سازمان باید آن را به مراجع مربوطه گزارش کند و پیگیری مدنی و کیفری یا اقدام حقوقی اداری به‌وسیله مراجع مربوطه را مدنظر قرار دهد.
- سازمان‌ها موظف‌اند با در نظر گرفتن مجازات‌های منسجم، پایبندی خود به سیاست‌های حفاظت از افشاگر را نشان دهند و کسانی که ممکن است به‌سمت رفتار آسیب‌زا در قبال افشاگران بروند را بازدارند.

- کسانی که متهم به رفتار آسیب‌زا، مداخله یا نقض محرمانگی می‌شوند، باید حق پاسخ‌گویی و کمک گرفتن (مشاوره) را داشته باشند.

پشتیبانی از افشاگران

سازمان‌ها وظیفه دارند افشاگران را از هرگونه آسیب به سلامت و حرفه مصون نگاه دارند.

افشاگری اغلب با ایجاد استرس و گاه ترس همراه است و یک اقدام زمان‌بر است؛ ازاین‌رو افشاگری می‌تواند روی کارکرد و سلامت افراد تأثیر منفی داشته و به آسیب‌های حرفه‌ای و زیان‌های مالی بینجامد. سازمان‌ها باید از رسیدن این آسیب‌ها به افشاگران پیشگیری کنند یا آن‌ها را به حداقل رسانند. در این راستا سازمان‌ها وظیفه دارند:

- پشتیبانی‌هایی مانند تغییر دادن مدیر بالادستی یا فضای کار، دسترسی به خدمات روانشناسی و مشاوره محرمانه را به افشاگران پیشنهاد کنند.
- تضمین کنند که افراد مسئول دریافت گزارش‌ها و ارتباط با افشاگران همچون مسئول افشاگری، مدیر بالادستی یا سرویس‌دهندگان بیرونی از آموزش‌های لازم برای شنونده بودن و ایجاد امنیت روانی برخوردار هستند.

حفاظت از افراد دخیل

سازمان‌ها باید از هویت و حقوق افراد دخیل صیانت کنند. برای نمونه هر سازمان باید مجازات‌های کارآمد، متناسب و بازدارنده‌ای را برای افرادی که عمدا اطلاعات نادرست گزارش می‌کنند در نظر گیرند.

فرد یا افرادی که در گزارش افشاگر مضنون به انجام تخلف معرفی شده‌اند نیز زیر چتر اقدامات حفاظتی قرار می‌گیرند.

فرد دخیل به کسی گفته می‌شود که در گزارش افشاگری مظنون بـه تخلـف یـا رفتـار آسیب‌زا، همکاری با چنین فردی توصیه گردیده است. فـرد دخیـل می‌توانـد حقیقـی یـا حقوقی باشد.

- هویت فرد دخیل باید مورد حفاظت قرار گیرد.
- در حین رسیدگی به هر گزارش، فرد دخیل بایـد بی‌گنـاه تلقـی شـود، از حـق پاسخ‌گویی و دریافت کمک بهرمند گردد و به همان شیوه به‌کاررفتـه در مـورد افشاگر، از هویتش حفاظت شود.
- سازمان‌ها بایستی برای کسانی که عمدا اطلاعات نادرسـت گـزارش می‌کننـد مجازات‌های کارآمد، متناسب و بازدارنده تعریف کنند.
  - سازمان‌ها حق ندارند در هنگام اشاره به گزارش‌هـای نادرسـتی کـه عمـداً ارائه شده‌اند، واژگـانی همچـون «بـدخواهی» و «سوءاسـتفاده» را بـه‌کار ببرند.
  - وظیفه اثبات اینکه افشاگر در زمـان ارائـه گـزارش از نادرسـتی اطلاعـات درون آن آگاه بوده، بردوش فردی است که این ادعا را مطرح کند.

نظارت و ارزیابی پیوسته

IWS باید دسته‌کم هر سال به شکل رسمی ارزیـابی گردیـده و در زمینـه بهبـود کـارایی، به‌روز بودن و همخوانی با مقتضیات قانونی و اجرایی، اصلاحات لازم در آن انجام پذیرد.

IWS بایستی به شکل پیوسته نظارت شده و به‌طور منظم ارزیابی و اصلاح گردد.

- سازمان‌ها باید معیارهایی برای نظارت کردن و برآورد کارایی و درستی سیستم افشاگری درونی تعریف کنند.

- ارزیابی از IWS می‌تواند به شکل درونی صورت پذیرد ولی لازم است ارزیابی‌های بیرونی مستقلی نیز روی آن انجام شود. این مهم توسط مسئولان دولتی، مشاوران کارشناس و یا سازمان‌های اجتماعی مورد تأیید سازمان به انجام می‌رسد.
- در ارزیابی از IWS باید طرف‌های مربوطه ازجمله کارکنان، اتحادیه‌های بازرگانی و دیگر نمایندگان کارکنان نقش داشته باشند.
- هیئت‌مدیره هر سازمان باید به شکل مرتب گزارش‌هایی از مسئول یا اداره افشاگری و رئیس سازمان پیرامون نتایج ارزیابی IWS دریافت نموده و به‌طور مستقل درستی و یا نادرستی آن را ارزیابی نماید.

برجسته‌ترین مسائلی که ارزیابی از سیستم افشاگری درونی باید به آن‌ها پاسخ دهد:

- پس از گذشت یک‌سال از به‌کار افتادن سیستم افشاگری درونی، آیا سازمان منابع انسانی یا مالی مشخصی در راستای کارایی بهتر به این سیستم اختصاص داده است؟
- آیا سازمان در زمینه اخلاق، پیروی از سیاست‌ها و سیستم افشاگری درونی، دپارتمان مشخصی ایجاد کرده است؟ اگر پاسخ منفی است، مسئول یا دایره افشاگری زیرمجموعه چه دپارتمانی شده است؟
- آیا میانگین زمانی پیگیری هر گزارش و دادن بازخورد به افشاگر سه ماه یا کمتر است؟
- آیا برای بازرسی درونی/ بیرونی از IWS برنامه‌ریزی صورت گرفته است؟ بازه زمانی تکرار آن چقدر است؟ چه نتایجی به‌دست‌آمده است؟
- آیا بازرسان سیستم افشاگری درونی، از سوی هیئت‌مدیره برگزیده شده‌اند؟

- آیا IWS از سوی مرجع شایسته‌ای مانند اداره مبارزه با فساد یا نهاد افشاگری ارزیابی گردیده است؟ نتایج چه بودند؟
- آیا در یک سال گذشته برای افشاگران احتمالی آموزش آگاهی بخش یا فعالیت آگاهی بخش دیگری در ارتباط با IWS انجام شده است؟
- در یک سال گذشته آیا برآوردی از میزان آگاهی و اعتماد در ارتباط با IWS صورت گرفته است؟ نتایج چه بودند؟
- در یک سال گذشته گزارشی دریافت کرده‌اید؟ چه تعداد؟
- در یک سال گذشته آیا گزارشی را پیگیری کرده‌اید؟ چه تعداد؟
- در یک سال گذشته آیا گزارش افشاگری یا شکایت از رفتار آسیب‌زا به اقدام انضباطی یا پیگیرد قانونی انجامیده است؟ چه تعداد؟
- آیا شیوه پیگیری سیستماتیکی برای تضمین حفاظت از اقدامات تلافی‌جویانه نسبت به افشاگران در گذر زمان وجود دارد؟ برای نمونه در بازه‌های زمانی شش ماهه، یک ساله یا دو ساله؟
- آیا سیستم افشاگری درونی به‌لحاظ فردی رویکرد فراگیر و مثبت نسبت به جنسیت دارد؟ آیا برای شناسایی و رسیدگی به الگوهای جنسی گزارش‌دهی و موانع گزارش‌دهی مانند رفتار آسیب‌زا، داده‌هایی گردآوری و تحلیل شده‌اند؟ در این صورت آیا هر دو جنس و فاکتورهای دیگری مانند تجربه‌های شخصی از گزارش‌دهی در این کار لحاظ گردیده‌اند؟
- آیا برای اصلاح بازرسی‌های دوره‌ای و گزارش‌های سالانه از IWS سازوکاری وجود دارد؟ زمان‌بندی آن چگونه است؟

منابع

منابع برگرفته از شفافیت بین‌الملل

1) Andy McDevitt and Marie Terracol (2020), *Assessing Whistleblowing Legislation: Methodology and Guidelines for Assessment Against the EU Directive and Best Practice*, Transparency International, www.transparency.org/en/publications/assessing-whistleblowing-legislation
2) Jacqueline de Gramont (2017), *The Business Case for "Speaking Up": How Internal Reporting Mechanisms Strengthen Private-Sector Organisations*, Transparency International, www.transparency.org/en/publications/business-casefor-speaking-up
3) Marie Terracol (2019), "Building on the EU Directive on Whistleblower Protection", Position Paper, Transparency International, www.transparency.org/whatwedo/publication/building_on_the_eu_directive_for_whistleblower_protection
4) Marie Terracol (2018), *A Best Practice Guide for Whistleblowing Legislation*, Transparency International, www.transparency.org/whatwedo/publication/best_practice_guide_for_whistleblowing_legislation
5) Transparency International (2013), International Principles for Whistleblowing Legislation, www.transparency.org/whatwedo/publication/international_principles_for_whistleblower_legislation
6) Peter Wilkinson (2017), *10 Anti-Corruption Principles for State-Owned Enterprises*, Transparency International, www.transparency.org/en/publications/10-anti-corruption-principles-for-state-owned-enterprises
7) Marie Chêne (2021), "Finding a voice, Seeking Justice – the barriers women face to reporting corruption in the European Union", Position Paper, Transparency International, www.transparency.org/en/publications/ findingvoice-seeking-justice-barriers-women-face-reporting-corruption-european-union
8) Transparency International Ireland (2021), *National Integrity Index 2021, Public-Sector Bodies (Part 1), Semi-States and Universities*, www.transparency.ie/resources/national-integrity-index/semi-state-universities-index- 2021/report
9) Dr Roland Gjoni (2021), *National Integrity Index 2020, Private Sector: Assessing Disclosure Practices of 30 Irish Companies*, Transparency International Ireland, www.transparency.ie/resources/national-integrity-index/privatesector-index/report-2020
10) Matthew Jenkins (2020), "Overview of whistleblowing software", U4 Helpdesk Answer, Transparency International, https://knowledgehub.transparency.org/helpdesk/overview-of-whistleblowing-software
11) TRANSPARENCY INTERNATIONAL

12) Nieves Zúñiga (2020), “Gender Sensitivity in Corruption Reporting and Whistleblowing”, U4 Helpdesk Answer, Transparency International, https://knowledgehub.transparency.org/helpdesk/gender-sensitivity-in-corruptionreporting-and-whistleblowing
13) Kaunain Rahman (2018), “The impact of General Data Protection Regulation on whistleblowing”, Transparency International, https://knowledgehub.transparency.org/ helpdesk/the-impact-of-the-general-data-protectionregulation-on-whistleblowing
14) Caitlin Maslen (2018), “Financial incentives for whistleblowers”, Transparency International, https://knowledgehub.transparency.org /helpdesk/financial-incentives-for-whistleblowers
15) Suzanna Khoshabi (2017), “Internal Whistleblowing Mechanisms”, Topic Guide, Transparency International, https://knowledgehub.transparency.org /guide/topic-guide-whistleblowing/4250

دیگر منابع:

1) International Chamber of Commerce (2022), Guideline on Whistleblowing, https://iccwbo.org/publication/icc- 2022-guidelines-on-whistleblowing/
2) International Organization for Standardization (ISO) (2021), Whistleblowing management systems — Guidelines, ISO 37002:2021
3) UNODC (2021), Speak Up for Health! Guidelines to enable whistle-blower protection in the health-care sector, www.unodc.org/documents/ corruption/ Publications/2021/Speak_up_for_Health_-_Guidelines_to_Enable_WhistleBlower_Protection_in_the_Health-Care_Sector_EN.pdf
4) OECD (2021), *Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions*, OECD/LEGAL/0378, www.oecd.org/corruption/2021-oecd-anti-briberyrecommendation.htm
5) Vigjilenca Abazi (2021), Guide to Internal Whistleblowing Channels and the Role of Trade Unions, Eurocadres, www.eurocadres.eu/publications/guide-internal-whistleblowing-channels-and-the-role-of-trade-unions
6) Kai-D Bussmann, Sebastian Oelrich, Andreas Schroth, Nicole Selzer (2021), *The Impact of Corporate Culture and CMS: A Cross-Cultural Analysis on Internal and External Preventive Effects on Corruption*
7) European Parliament and Council of the European Union (2019). *Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law*, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L1937
8) European Data Protection Supervisor (2016), Guidelines on processing personal information within a whistleblowing procedure, https://edps.europa.eu/ data-protection/data-protection/referencelibrary/whistleblowing_en

9) Protect (2022), *Prescribed Persons – Annual Whistleblowing Reports: Best Practice Guide, https://public-concern-atwork.s3.eu-west-1.amazonaws.com/wp-content/uploads/images/2022/08/30095958/Annual-Whistleblowing-ReportsBest-Practice-Guide.pdf*