How Employers Can Prevent Workplace Technology-Facilitated Abuse

What is Technology-Facilitated Abuse?

Tech-facilitated abuse (TFA) is the use of technology to monitor, control, harass, stalk, impersonate, or harm another person. In workplace contexts, this can include unauthorized access to work accounts, tracking location through company vehicles or phones, or sending harassing messages through work email or collaboration tools.

What does Workplace TFA Look Like?

TFA in the workplace can look like an employee perpetrating harm against other employees. The employee may have a legitimate need to access some workplace systems, making it difficult to identify what constitutes misuse. Power dynamics—especially if the person causing harm is a supervisor—can also add complexity when the employee experiencing TFA wishes to report the abuse.

Examples of Workplace TFA by a Coworker or Supervisor

- **Inappropriate surveillance through workplace software:** Using shared drives, calendars, or project management tools to monitor other employees' activities beyond work purposes
- **Misusing administrative access:** A supervisor accessing an employee's email, files, or communications without legitimate business need
- **Using monitoring tools for personal purposes:** Accessing "bossware" data to track an employee's location or activity for non-work reasons
- **Inappropriate contact:** Sending harassing messages through work email, Slack, or other platforms
- **Weaponizing work systems:** Manipulating schedules, assignments, or access privileges as a form of control

FUTURES WITHOUT VIOLENCE®

WORKPLACES RESPOND TO DOMESTIC & SEXUAL VIOLENCE
A NATIONAL RESOURCE CENTER

What is Tech-Facilitated Abuse?, cont.

Workplace TFA can also look like an employee's intimate partner – who does not work at your organization – using technology to abuse, monitor, or harass the employee through your workplace systems.

Examples of Workplace TFA by an Employee's Current or Former Intimate Partner

- **Constant contact with the employee or their co-workers:** Flooding their work email, phone, or messaging apps with calls, texts, or messages.
- **Image-based abuse:** Sending intimate images (real or AI-generated) to the employee's supervisor, coworkers, customers, or organizational partners.
- **Impersonation:** Accessing the employee's work accounts to send messages as them or creating fake accounts in their name.
- **Location tracking:** Monitoring the employee's location through a company phone, vehicle GPS, or badge access records.
- **Schedule surveillance:** Accessing the employee's work calendar to know where they'll be and when.
- **Account compromise:** Logging into the employee's work email, Slack, or other accounts to read their messages or monitor their communications.

These behaviors negatively impact an employee's safety and security, and can also affect their professional reputation and relationships. These are acts of employment sabotage, which is a form of economic abuse as it can harm an employee's ability to maintain steady employment and achieve future economic mobility.

About this toolkit
This toolkit was developed by Futures Without Violence. This project is supported by Grant No. 15JOVW-24-GK-06128-NRCW awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed on this toolkit or in any materials on this site, are those of the authors and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.

For questions or technical assistance, fill out our Training & Technical Assistance form.

Why Employers Should Address Workplace Technology-Facilitated Abuse (TFA)

Domestic violence costs U.S. employers an estimated $8.3 billion annually in lost productivity, healthcare costs, and turnover. Beyond the business case, employers have ethical and often legal obligations to provide safe workplaces.

78% of intimate partner stalkers used workplace resources at least once to contact their target.[1] If someone within your organization is misusing workplace equipment to cause harm or if an outside entity has exposed a vulnerability in the system, correcting this as soon as possible ensures a safer workplace environment for all workers.

When TFA interrupts the workplace, employers can incorrectly identify the person experiencing the abuse as the security risk or as a "distraction" and penalize the person experiencing the abuse. When this happens, employers can inadvertently contribute to the employment sabotage of the survivor, leaving them further isolated and at risk.

Key Elements of Effective Workplace Responses to TFA

- **Designated liaison:** A trained point of contact for employees experiencing domestic violence, sexual assault, or stalking (DVSAS).
- **Safety planning:** Procedures for collaborating with local advocates to develop individualized workplace safety plans.
- **Confidentiality protections:** Clear limits on who needs to know about an employee's situation.
- **Decentralized technology security infrastructure:** Partnering with a third-partner organization that provides network security services to a company, de-centralizing control over employer-provided devices and software ensures that crucial business functions, like data and device management, are not being misused by an employee or department because of reduced accountability.
- **Leave and accommodations:** Provisions for time off and reasonable accommodations for survivors, including support documenting abuse.
- **Non-discrimination:** Clear language in all policies that survivors will not be discriminated or retaliated against because of their experience of harm.
- **Training:** Regular training for HR, supervisors, and all employees on recognizing and responding to DVSAS, including TFA.

[1] https://www.maine.gov/labor/labor_stats/publications/dvreports/domesticoffendersreport.pdf

How Employers Can Prevent Workplace Technology-Facilitated Abuse (TFA)

While every workplace is unique with its own culture, values, and practices, no workplace is exempt from the impacts of domestic violence, sexual assault, and stalking (DVSAS). An employer has a duty to maintain a safe and respectful workplace where everyone is welcome and able to thrive. This is not possible when the impacts of DVSAS go unaddressed.

Responsive policies can save lives. Policies that address DVSAS are critical to creating safer workplaces. An effective DVSAS policy can mitigate preventable threats to the workplace and ensure survivors feel supported and are not further isolated or harmed by the perpetrator's actions.

Employers can revise their workplace policies to address TFA in addition to DVSAS, including all the ways in which they intersect. Below are samples of model policy language as well as definitions that can be included in workplace policies to better inform employees.

Model Policy Language

The following language is from the Workplaces Respond Guide to Create a DVSAS Policy *(Futures Without Violence, 2025)*:

Use of Workplace Equipment or Resources to Document Instances of DVSAS

[Employer] recognizes individuals surviving DVSAS may be subject to surveillance and intrusive monitoring of their personal devices.

[Employer] further recognizes that an individual covered by this policy may need to use workplace equipment and resources to document instances of violence that they are experiencing either within or outside of the world of work. Reasonable use of workplace equipment or resources in this way will not be considered misuse of workplace equipment or resources.

[Employer] will not retaliate against an individual covered by this policy or deprive that individual of employer-issued equipment because the individual used employer-issued equipment to document an instance of DVSAS committed against the covered individual or a family member of that individual.

[Employer] shall grant an employee access to any photographs, voice or video recordings, sound recordings, or any other digital documents or communications stored on an employer-issued device relating to DVSAS.

How Employers Can Prevent Workplace Technology-Facilitated Abuse, cont.

This policy does not prohibit [Employer] from complying with an investigation, court order, or subpoena for a device, information, data, or documents. Furthermore, this policy does not relieve an employee's obligation to comply with an employer's reasonable employment policies or to perform the essential functions of employment.

Prohibition on Misuse of Workplace Equipment to Facilitate Abuse

[Employer] does not tolerate, and will not tolerate, any perpetration of DVSAS done by an individual covered by this policy. [Employer] expressly prohibits the use of any workplace equipment, resources, or benefits to perpetuate or further DVSAS.

If [Employer] receives information that alleges or suggests an individual covered by this policy has engaged in an incident of DVSAS, including the use of workplace equipment, resources, or benefits, the matter shall be referred to [Employer Designee] for the purpose of investigating the information or allegation received.

For Co-Workers Who Observe Misuse of Workplace Equipment

If individuals covered by this policy observe inappropriate surveillance or the misuse of workplace equipment or resources to perpetrate DVSAS, they shall report what was witnessed to [Employer Designee] as soon as practicable. Reports of this nature will be kept confidential to the best of [Employer]'s ability.

Acknowledgements:
Workplaces Respond extends its deepest gratitude to Lana Ramjit at the National Resource Center on Cybercrimes, Julia Holtemeyer at the Stalking Prevention Awareness Resource Center, and Chris MacDougall at Futures Without Violence for their consultation and support in the creation of this resource.

WORKPLACES RESPOND
TO DOMESTIC & SEXUAL VIOLENCE
A NATIONAL RESOURCE CENTER

Workplaces Respond provides technical assistance to workplace stakeholders seeking to better prevent and respond to domestic violence, sexual assault, stalking, and harassment impacting the workplace.

Scan this QR code to access the Resource Center.