MANAGING A POST-COVID RESURGENCE OF EMPLOYEE MISCONDUCT CASES

處理疫情後捲土重來的員工不當行為

MATTHEW DURHAM
Registered Foreign Lawyer
Gall Solicitors

高嘉力律師行
註冊
外地律師

DAVIN TEO
Head of Forensic Technology Asia
Alvarez & Marsal

安邁企業諮詢亞洲區法證科技團隊負責人張章維

FELDA YEUNG
Of Counsel, Gall Solicitors

高嘉力律師行
資深顧問律師
楊芷彤

Employee misconduct can take many different forms, be it financial, regulatory, harassment, discrimination, or breaches of company policies. Allegations and complaints regarding misconduct or the discovery of incidences of misconduct may come from a variety of sources and functions, ranging from routine compliance checks to external sources, whistleblowers or even regulatory dawn raids.

How to protect the organisation

Companies should ensure that they have solid employment documentation, policies and procedures in place, including employment contracts; employee handbooks and policies; a code of conduct; a whistleblower policy; and, particularly following the impact of COVID-19 on work practices, a bring-your-own-device and/or IT use policy as well as a work-from-home policy. Obligations and standards must be reinforced through regular training and communications.

How to define the investigation's objectives and weigh considerations

If, despite stringent measures in place, a case of misconduct is unveiled, consideration must be given to the underlying purpose and aim of an investigation before embarking on the process.

The employer should question:

- Are the issues or allegations credible and do they require a full investigation?
- Will the financial cost outweigh the damage caused/loss incurred?
- Is there a reputational risk, and how to manage it?
- How to manage the pressure on resources?
- How will it affect staff morale and leadership?
- Does it involve cross-border data transfer?

How to prepare for an investigation

It is important to meticulously plan investigations by considering which departments to involve – legal, compliance, HR, IT, forensics,

員工不當行為可以有很多種，涉及範圍包括財務、監管、騷擾、歧視或違反公司政策。企業可通過各種消息來源和途徑，包括例行合規檢查、外部消息來源、舉報人、甚至監管機構的「黎明突襲」行動，接獲關於不當行為的指控和投訴，或揭發不當行為。

如何保障企業

企業應確保齊備僱傭文件、政策和流程以保障公司，包括僱傭合約、員工手冊和政策、行為準則、舉報政策；尤其鑑於新冠疫情對工作模式的影響，亦應制定自攜設備和/或資訊科技應用政策，以及在家工作政策。企業必須進行定期培訓和溝通，以確保員工遵守相關規定和準則。

如何定義調查目標並權衡考慮

除了制定嚴格的措施，一旦發現不當行為，展開調查前須先考慮調查的基本目的和目標。

僱主應質疑：

- 提出的問題或指控是否可信？是否需要進行全面調查？
- 財務成本會否超過造成的損害/損失？
- 是否存在聲譽風險，如何處理？
- 如何管理資源壓力？
- 這對員工士氣和領導管治將有何影響？
- 是否涉及跨境數據轉移？

如何準備調查

必須就調查進行細心規劃，考慮涉及的部門 — 法律、合規、人力資源、資訊科技、法證、管理、總部等，決定由誰統籌調查，確定相關司法管轄區，並檢查要為受查員工提供的文件。

內地分別由2021年9月1日和2021年11月1日起實施新《數據安全法》和《個人信息保護法》，這將影響日後所有涉及內地的跨境調查。兩條法例均規定必須得到「中華人民共和國監管部門」批准才能將數據轉移

到內地以外地區，企業和法律與法證顧問需了解如何在新監管框架下運作。

如何展開法證調查

法證調查人員是受過訓練的科技專家，他們與企業及其法律顧問攜手合作，在調查期間收集、保存和分析數據。

單靠企業內部資訊科技部門處理可能對調查至關重要的證據，或會增加處理不當、篡改和損壞的風險。僱主必須考慮何時啟動法證調查程序，並搜集所有適用的相關數據和設備。

要取得最佳成果，調查必須具針對性、有組織、保密和謹慎，並盡量避免搜證過程妨礙業務運作。若數據儲存在雲端系統上，可在工作時間以外秘密搜證，或在某些情況下遙距進行相關操作。

監管機構進行「黎明突襲」行動期間，一般會搜集特定交易和個人的數據，法證調查人員將會與法律顧問和監管機構協商收集數據的最佳方式，以盡量減少對業務的干擾。

進行面談並作出跟進

要取得最佳成果，必須在多方面作出策略和務實決定，包括受訪者和證人的身份；面談的時間和地點，一般會遠離辦公場所；首席訪談員和其他與會者；以及牽涉的部門。有系統的調查程序和清晰的提問也有助調查取得成果。

面談後採取的具體行動，因面談結果而定。可行的步驟包括：與員工就調查狀態、保密協議和持續配合進行溝通；要求員工停職或放有薪假；即時歸還公司設備、硬盤和禁止遙距登入公司系統；即時解僱。僱主亦可考慮加強公司和大廈出入口保安。

因情況而異

員工不當行為個案各有不同，沒有統一適用的調查方式。企業應時刻做好對策準備，與所有持份者進行清晰的溝通，並與外部法律顧問、法證科技專家和公關專家等關鍵聯繫人保持聯繫。

management, HQ; identifying who will lead and co-ordinate the investigation; determining relevant jurisdictions; and checking what documentation is in place for the employee to be investigated.

The new Data Security Law effective from 1 September 2021 and the Personal Information Protection Law enforced from 1 November 2021 will impact all cross-border investigations involving Mainland China in the future. Both require approval from "competent authorities of the PRC" to transfer data outside of Mainland China and companies and legal and forensic advisers will need to learn how to operate within this new regulatory framework.

How to lead a forensic investigation

Forensic investigators are technology experts trained to collect, preserve, and analyse data during an investigation. They work hand-in-hand with companies and their legal advisers.

Relying on in-house IT departments only could increase the risk of mishandling, tampering and corruption of evidence that may be vital to the investigation. Employers must consider when to launch the forensic investigation, and gather all available and relevant data and devices.

For best results, investigations must be targeted, organised, confidential and discreet. Forensics operate to minimise disruption to the business. Collections can be done covertly outside business hours, or remotely in some instances, when data is stored in the cloud.

In regulatory dawn raid situations, regulators are generally looking for data on specific transactions and individuals and forensic investigators will co-ordinate with legal advisers and regulators to negotiate the best data collection strategy to minimise interruption.

Conducting and following up on interviews

Several strategic and practical decisions must be made concerning the identity of interviewees and witnesses; timing and location of interviews – generally away from office premises; the lead interviewer and others in attendance; and departments involved. A structured process and clear questioning are also key to a fruitful investigation.

The course of action to take after the interview may vary significantly depending on the interview outcome. Possible steps include: communication with the employee regarding status of the investigation, confidentiality obligations and need for ongoing co-operation; suspension or garden leave; immediate return of company devices, hard drives and remote log-in capability; immediate termination of employment. Employers may also consider enhancing security and access to the building.

No one-size-fits-all

There is no one-size-fits-all when it comes to employee misconduct cases, but companies should always be prepared and strategic, communicate clearly with all stakeholders, and have key contacts, including external legal counsel, forensic technology experts and public relations experts, readily available.