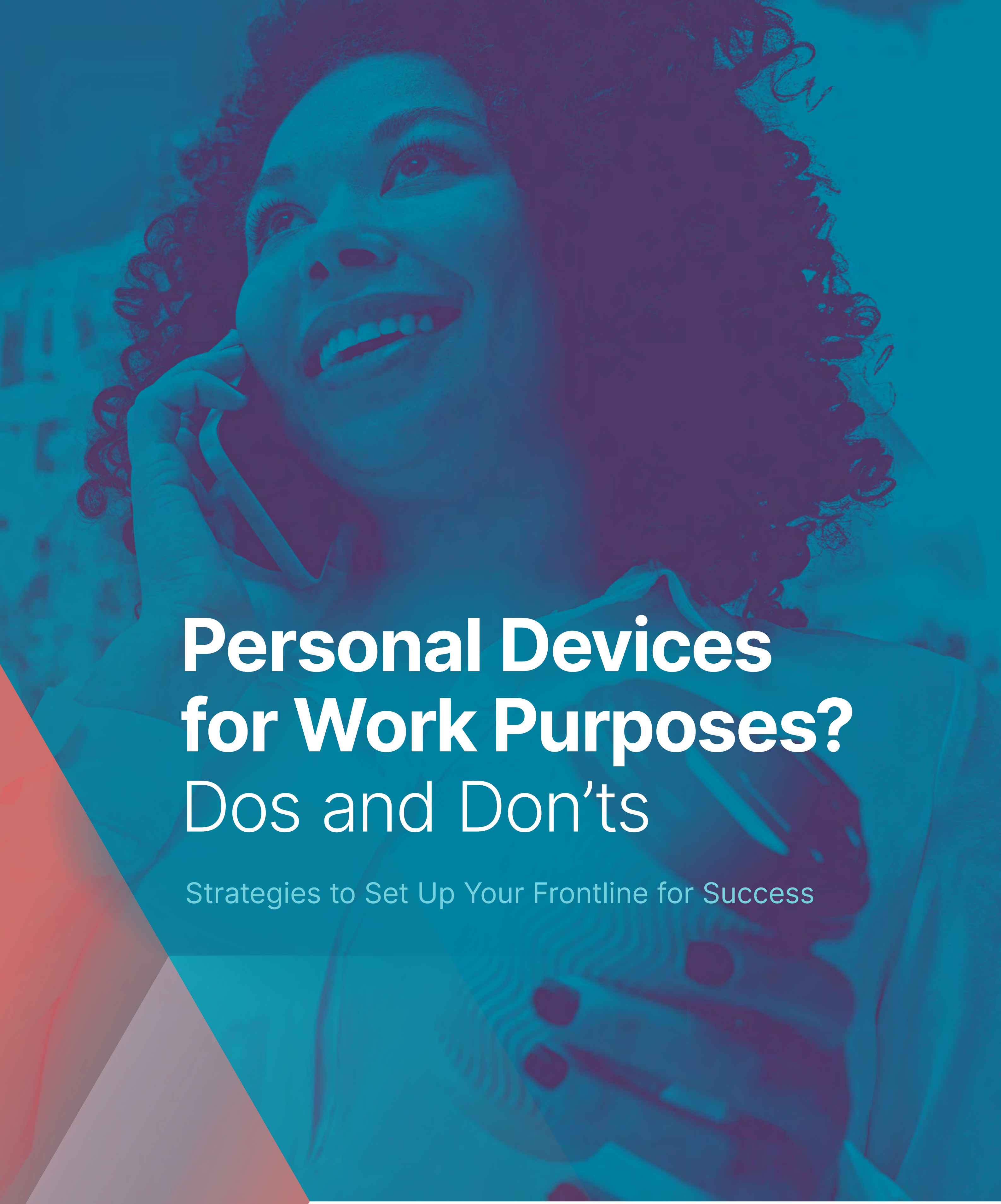


Personal Devices for Work Purposes? Dos and Don'ts

Strategies to Set Up Your Frontline for Success

BEEKEEPER

In today's interconnected world, the lines between work and personal life are becoming increasingly blurred.

With the rise of workplace technology that keeps us all connected, employees are often expected to remain digitally accessible even outside of traditional working hours. This shift has prompted discussions around compensating employees for their offline use of communication and collaboration platforms, such as Beekeeper. As organizations grapple with the complexities of modern work arrangements, it has become imperative to think about the following questions:

- **Is company data secure on a personal device?**
- **How do we support personal devices?**
- **Do we have to provide compensation for the use of personal devices or not?**

Addressing these issues will ensure fair treatment of employees and compliance with evolving labor laws.

The Always-On Dilemma: **Managing BYOD, Offline Work, and Fair Pay for Frontline Teams**

Frontline employees are the backbone of an organization's success. But what happens when the workday bleeds into personal time?

The rise of Bring Your Own Device (BYOD) programs and the constant connectivity it fosters can blur the lines between work and personal life for frontline workers. This creates a crucial challenge: ensuring clear communication and efficient operations while guaranteeing a good work-life balance for employees.

Purpose and Scope

Use this eBook as a comprehensive guide that delves into the complexities of BYOD, offline work, off-the-clock compensation, and risk tolerance for frontline teams, and learn insights and strategies to better understand the current state of the market and its evolving landscape. By examining customer perspectives, legal requirements, best practices, and Beekeeper's recommended solutions, organizations can define an action plan to address the challenges and opportunities associated with leveraging BYOD and technologies for their frontline teams.

Table of Contents

State of the Market: **Trends in Offline Compensation**

The landscape of compensation for offline use of communication and collaboration platforms continues to evolve considering shifts in employee engagement practices and workforce management processes, dynamic labor laws and regulations, and expectations of work-life balance.

This is even more compounded for frontline organizations and the unique needs of managing a deskless workforce. **Organizations across frontline industries are increasingly recognizing the importance of compensating employees for their time spent engaging with work-related tasks outside of traditional working hours.**

This trend is driven by factors such as the growing prevalence of remote work, the blurring of boundaries between work and personal life, and the need to ensure fair treatment of employees.

Labor Laws and Compliance

Compliance with labor laws, particularly in regions like California with stringent regulations, is a critical consideration for organizations implementing offline compensation with BYOD policies.

Similar trends are emerging in other regional and global geographies, indicating a broader shift towards greater scrutiny of employer practices regarding compensation and work-life balance.
Compensation practices set forth by organizations will need to consider regional impacts, laws, and compliance. By aligning with labor laws, organizations foster trust and fairness in the workplace.

California and Off-the-Clock Work: Stricter Standards

California adheres to stricter standards regarding off-the-clock work for hourly employees compared to federal regulations. California's labor laws, including requirements for minimum wage, overtime pay, and reimbursement for business expenses, have significant implications for how organizations approach compensating employees for their offline use of communication platforms. Any work-related communication (excluding shift-filling or absence notifications) – even brief email exchanges or short phone calls – likely qualifies as compensable work time under California law.

Unlike most states, California requires employers to reimburse employees for business calls and data usage on their personal phones, even if the use is simply allowed, not mandatory. This can be a hurdle for some organizations considering BYOD programs. Some California employers address this by offering a small monthly stipend to help offset phone usage costs.

Definitions:
BYOD vs. MDM

Bring Your Own Device
BYOD

BYOD refers to a policy allowing employees to use their personal electronic devices, such as smartphones, tablets, or laptops, for work-related tasks. This approach enables employees to use devices they are comfortable with, potentially increasing productivity and flexibility.

However, it also poses security and privacy risks for organizations, as personal devices may not meet corporate security standards and is also dependent on appropriate, acceptable owner behavior and usage.

Mobile Device Management
or Managed Devices – MDM

MDM encompasses the provision, deployment, company ownership, and management of both hardware and software solutions used to secure and control mobile devices within an organization.

This includes not only implementing software solutions for managing and securing mobile devices but also aspects such as device provisioning, configuration, inventory management, and remote troubleshooting. Because devices are owned and regulated by the company, MDM enables IT administrators to enforce security policies, control access to corporate data, and remotely manage devices, ensuring compliance with organizational standards and regulations throughout the entire lifecycle of the mobile devices.

Benefits

BYOD	MDM
Familiarity: Workers use devices they are comfortable with, potentially increasing productivity and satisfaction. This also means less time training employees as they already know how to use their own devices, further enhancing productivity.	**Control:** Organizations can enforce security measures and manage updates more efficiently, mainly through an MDM solution.
Flexibility: BYOD enhances information access and communication outside traditional work hours, such as checking shift schedules or pay stubs. New employees can easily integrate and join in on conversations and company culture right away during onboarding.	**Uniformity:** Eases the integration of corporate applications, facilitates training, and promotes fairness.
Cost Savings: Companies can experience reduced hardware expenditure and maintenance costs. Organizations benefit from faster adaptation of new technologies as personal devices are typically kept up to date.	**Security:** Lower risk of data breaches and unauthorized access to corporate resources.
Security Risks: Personal devices introduce varied security vulnerabilities, complicating the enforcement of robust IT security policies.	**Cost:** The initial investment, maintenance, and replacement costs can be substantial.

Challenges

Privacy Concerns: Balancing company access and monitoring with employee privacy on personal devices can be complex.	**Device Provisioning and Management:** The logistics of provisioning, tracking, and managing a fleet of devices can be complex and resource-intensive.
Legal and Compliance Issues: Ensuring that BYOD practices comply with data protection regulations and industry standards requires careful policy crafting	**Less Flexibility:** Workers might have restricted access to devices outside work hours.
Compatibility Issues: Diverse devices may result in compatibility challenges with corporate applications.	**Risk of Loss or Damage:** The risk associated with device loss or damage can lead to additional expenses.
Management Complexity: Overseeing a wide array of personal devices can become cumbersome for IT departments.	**Hygiene and Sharing Concerns:** Especially relevant in shared device scenarios or health-sensitive environments, raising the need for strict cleanliness protocols.

Challenges and Risks

Understanding Legal Complexities and Compliance Requirements

One of the primary challenges organizations face when addressing offline compensation is navigating the complex landscape of labor laws and compliance requirements. California's labor laws, in particular, impose strict regulations on issues such as minimum wage, overtime pay, and reimbursement for business expenses. Ensuring compliance with these laws while developing offline compensation policies requires careful consideration and expertise in labor law.

Risks Associated when considering BYOD vs. MDM

The choice between Bring Your Own Device (BYOD) policies and Mobile Device Management (MDM) solutions presents organizations with various risks and considerations. BYOD policies offer flexibility and cost savings but raise concerns about data security, privacy, and fair compensation for off-duty use of personal devices. MDM solutions provide greater control over device management and security but may incur additional costs and logistical challenges. It is important for companies to assess the needs of their business, as well as impact and expectations for employees. Organizations must carefully weigh these risks and considerations when developing their offline compensation strategies.

HR Perspective

Human Resource teams have special considerations when it comes to risks related to pay and compensation calculations. Implementing BYOD policies introduces risks related to pay and compensation calculations for off-duty work. With employees accessing work-related tasks on personal devices, accurately tracking and compensating for this time becomes challenging. HR departments must navigate complex labor laws and regulations to ensure fair compensation for off-duty work, including overtime pay and reimbursement for business expenses. Failure to accurately calculate compensation for off-duty work can lead to legal liabilities, employee dissatisfaction, and compliance issues.

IT Perspective

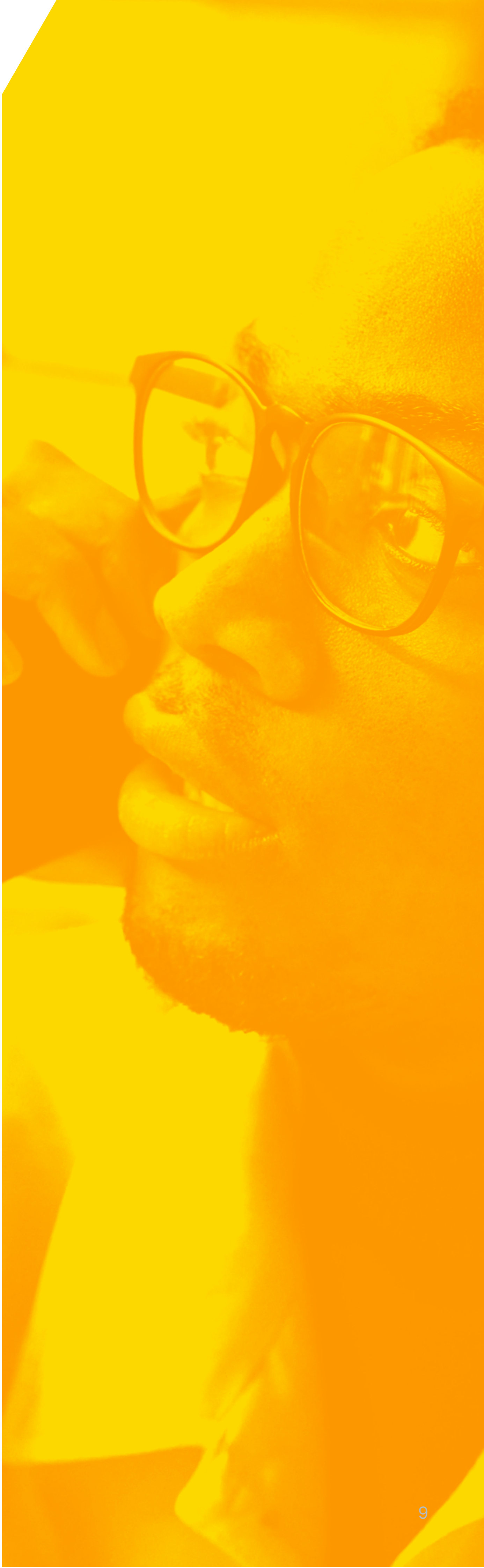
“Access to Intellectual Property (IP)” is an important topic for IT teams to define when implementing BYOD policies poses risks related to uncontrolled access to intellectual property. Allowing employees to access sensitive company data and resources on personal devices increases the risk of unauthorized access, data breaches, and IP theft. Without proper controls and security measures in place, IT departments may struggle to enforce policies and safeguard confidential information. Additionally, the use of personal devices for work purposes may introduce compatibility issues, software vulnerabilities, and challenges in maintaining security standards across diverse device types and operating systems.

Privacy Concerns and Employee Engagement

Implementing offline compensation policies, particularly those involving geo-fencing or location tracking, can raise privacy concerns among employees. Employees may feel uncomfortable with the idea of their employers tracking their whereabouts or monitoring their off-duty activities. This can lead to a decline in employee engagement and morale, undermining the effectiveness of offline compensation policies. Balancing the need for fair compensation with respect for employee privacy is essential for fostering a positive work environment and maintaining employee trust.

Impact of California’s Labor Laws and Implications in Other Regions

California’s stringent labor laws serve as a bellwether for broader trends in labor regulation and enforcement. As other regions follow suit with similar legislation, organizations operating outside of California must prepare for potential changes in labor laws and compliance requirements. Failure to adapt to these evolving regulatory landscapes can expose organizations to legal risks, financial penalties, and reputational damage.



Recommendations and Best Practices

Whether your organization chooses a BYOD program or opts for entirely Managed Devices, establishing robust security policies and best practices is paramount. Here are some key recommendations to consider for securing your system's access points, regardless of the device type.

Developing BYOD Policies

Organizations should develop clear and comprehensive BYOD policies that outline acceptable use guidelines, compensation practices, and privacy protections for employees. BYOD policies should address key considerations such as reimbursement for business expenses, off-duty use of personal devices, and data security requirements. By establishing transparent and fair BYOD policies, organizations can ensure compliance with labor laws and regulations while fostering a positive work environment. » Example BYOD Policy

Mitigating Risks and Ensuring Compliance

Organizations should take proactive steps to mitigate risks associated with offline compensation and ensure compliance with labor laws and regulations. This includes conducting regular audits of offline compensation practices, monitoring legal developments, and seeking guidance from legal experts when necessary. By staying informed and proactive, organizations can minimize legal risks, protect employee rights, and maintain compliance with applicable regulations.

Optimizing Engagement and User Experience

To maximize the effectiveness of offline compensation policies, organizations should prioritize user engagement and experience. This includes providing training and support to employees on how to use company sponsored apps effectively, soliciting feedback on user experience, and continuously iterating and improving the platform based on user input. By prioritizing user engagement and experience, organizations can drive adoption of offline compensation policies and ensure that employees derive maximum value from the platform.

Leveraging Industry Best Practices

Organizations should leverage industry best practices and benchmarks to inform their offline compensation strategies. This includes benchmarking compensation practices against industry peers, staying abreast of emerging trends and innovations, and learning from successful case studies and examples.

By adopting industry best practices, organizations can enhance the effectiveness and efficiency of their offline compensation policies and stay competitive in the marketplace.
Regardless of whether you choose a Bring Your Own Device (BYOD) program or opt for Managed Devices for your frontline employee communications app, security is crucial. A few best practices to consider for secure device access:

- **Authentication:** Encourage strong passwords and Multi-Factor Authentication (MFA) for all users, on both BYOD and managed devices. When considering employee app solutions, look for SSO and managed login solutions such as personalized QR code invitations.

- **Data Sensitivity:** When creating your organization's policies, identify any sensitive information (e.g., employee records, customer data) that should not be stored locally on personal devices under a BYOD program.

By addressing these key areas, you can ensure a secure environment for your frontline employee communications app, regardless of the device access method chosen.

Beekeeper's Approach and Solutions

Beekeeper offers a comprehensive suite of features and functionalities designed to help organizations address the challenges establishing BYOD policies and off-the-clock compensation.

Beekeeper's experience with a vast customer base and over half-a-million users using the Frontline Success system daily within their frontline organizations ensures that organizations have the tools they need to navigate the complexities of BYOD while ensuring compliance with labor laws and regulations.

Key Features and Functionalities

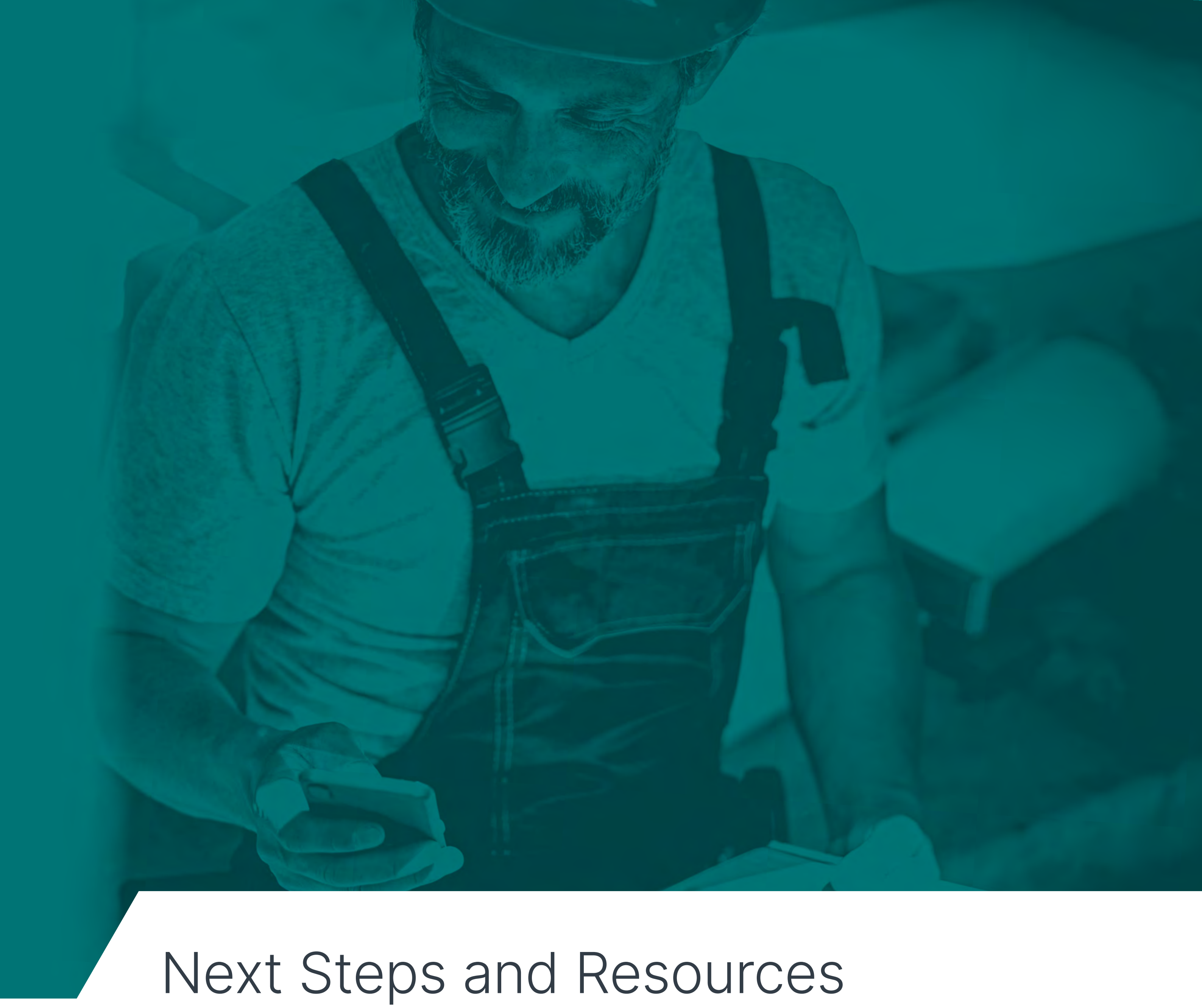
Fair Play Rules: Beekeeper enables organizations to establish fair play rules that define acceptable use policies for off-duty communication. These rules help organizations ensure that employees are compensated appropriately for their time spent engaging with work-related tasks outside of traditional working hours. Consider adding the following practices to strengthen fair play rules:

- Define off the clock-work in simple to understand terms and have employees sign a statement when they start using Beekeeper that states that the company does not expect them to, nor do they allow, off the clock work.
- Integrate a signed acknowledgement that no off the clock work was performed when hourly employees approve their time sheets for the week. Set up workflows within Beekeeper to automate and store signed documentation for easy reference by HR teams to ensure compliance.

Integration with Workforce Management Systems: Beekeeper seamlessly integrates with leading workforce management systems, such as UKG Ready, to streamline processes and ensure accurate tracking of employee time and attendance. This integration enables organizations to automate offline compensation calculations and ensure compliance with labor laws and regulations.

Do Not Disturb (DND) Feature: All Beekeeper users have the ability to mute notifications, allowing them to discourage communication during off-duty hours. Users can choose to mute all Beekeeper notifications or selectively mute notifications for certain streams. Additionally, managers can set up an Availability Status subheading in 1:1 chats to provide employees with up-to-date information about their coworkers' availability status before sending messages.

Consultative Support and Guidance: Beekeeper provides consultative support and guidance to organizations navigating offline compensation challenges. From developing BYOD policies to implementing fair play rules and a good do-not-disturb culture, Beekeeper's team of experts works closely with organizations to tailor solutions to their unique needs and requirements.



Next Steps and Resources

Taking Action: Implementing a Secure and Compliant Solution

Moving forward with BYOD policy can offer significant benefits for both your organization and your employees. However, ensuring a secure and compliant program requires careful planning and execution.

Here’s a breakdown of key action steps to get you started:

Review and Audit

- Existing BYOD Policies: Conduct a comprehensive review of your current BYOD policies (if any) to identify gaps and ensure alignment with the new program’s goals.
- Offline Compensation Practices: Analyze existing practices for compensating off-the-clock work, particularly how they might be impacted by BYOD communication. Consider consulting timekeeping and payroll specialists to identify areas for improvement.

Legal Compliance

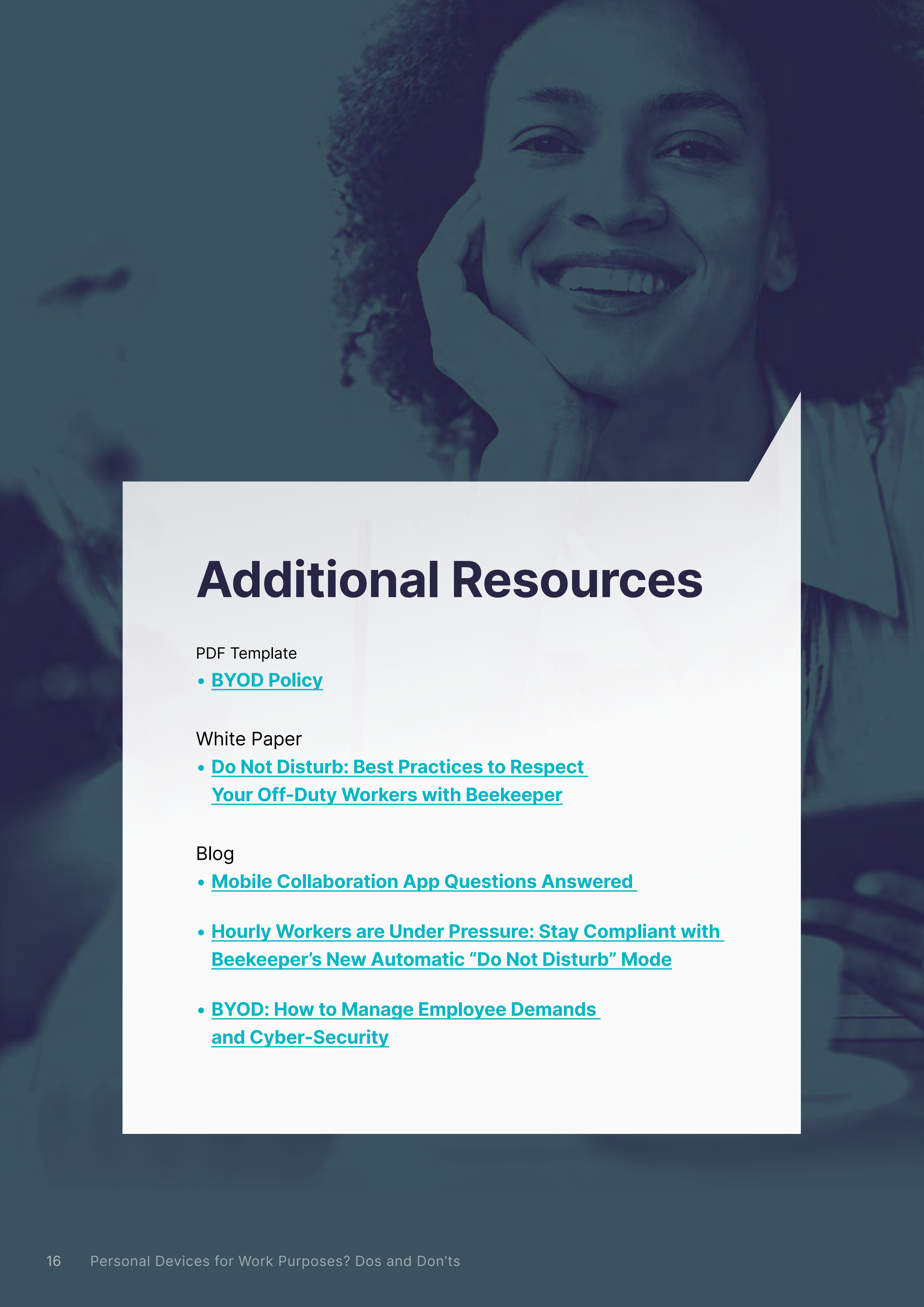
- Engage Legal Counsel: Partner with legal experts specializing in employment law to ensure your BYOD policy complies with all relevant federal and state regulations regarding off-the-clock work and data privacy.

Leveraging Technology

- Implement Beekeeper Features and Expert Best Practices: Explore and implement Beekeeper’s functionalities specifically designed to address potential BYOD-related topics. For instance, features like DND and notification settings, scheduling posts, and read receipts can help clarify expectations and set boundaries around work communication outside of regular hours.

Stakeholder Engagement

- Employee and Management Feedback: Solicit feedback from employees and relevant stakeholders (e.g., frontline managers, HR) throughout the BYOD implementation process. Conduct surveys, workshops, or focus groups to gather valuable insights and concerns.
- Iterative Policy Development: Use the gathered feedback to refine and improve your BYOD policy over time. This collaborative approach can help ensure the policy is practical, user-friendly, and addresses the needs of all parties involved.



Additional Resources

PDF Template

- BYOD Policy

White Paper

- Do Not Disturb: Best Practices to Respect Your Off-Duty Workers with Beekeeper

Blog

- Mobile Collaboration App Questions Answered
- Hourly Workers are Under Pressure: Stay Compliant with Beekeeper's New Automatic “Do Not Disturb” Mode
- BYOD: How to Manage Employee Demands and Cyber-Security

Congratulations to the entire company
Yesterday we have been awarded as one of the top 10 workplaces in the country. I want to thank everyone who made this happen!

Hey Adam, congrats on winning Employee of the Month! And thank's again for your referral. That was really a perfect match for our department.

Reception check-ins and customer service.

This is **Beekeeper**

Beekeeper is transforming the way frontline businesses work. Our mobile-first platform helps companies ditch paper and manual processes to improve employee engagement, retention, and performance.

Empower employees with direct access to the people, processes, and systems they need to do their best work. Companies around the world use Beekeeper to connect their teams, unify their systems and drive their businesses forward.

Ready to equip your workforce with a system they'll actually use?

» Schedule Time with one of our Frontline Experts

Zürich | San Francisco | Berlin | Krakow

BEEKEEPER