# Work From Home Guide

## Contents


# Welcome to Lithia & Driveway

Working remotely offers flexibility and convenience, but it also comes with responsibilities. As a remote team member, you are expected to maintain the same level of professionalism, productivity, and accountability as in a traditional office setting. Clear communication, meeting deadlines, and adhering to company policies are key to your success.

To ensure you have everything you need, please review the **Employee Handbook** and **New Team Member Guide**. These resources outline company policies, expectations, and important procedures to help you navigate your role. If you have any questions, reach out to your manager or your HR Business Partner (HRBP) for guidance.

# Resources for Work-From-Home Employees

Spark is where to turn when you need to find answers, forms, assistance, or information regarding all things Lithia & Driveway—

- Access **Workday** and all its apps for your employment needs
- Find quick links to learn more about your long list of **Total Rewards**
- Explore Employee Resources for important resources, including the **Employee Handbook**
- Request technical assistance via the **Request & Resource Center**
- Find the forms, policies, guides, and store materials from **DocXplorer**
- Broaden your professional horizons with free training courses in the **Learning Center.**
- Book travel and resolve expenses in **Concur**


# Company Policies & Procedures for Remote Work

## Work Hours & Availability

- Maintaining a consistent and professional schedule is essential for productivity and collaboration. Employees should align their work hours with their team's expectations and ensure availability during core business hours. Regular check-ins, responsiveness to emails and messages, and active participation in meetings help maintain effective communication and teamwork.
- If you need flexibility in your schedule, discuss expectations with your manager to ensure alignment with business needs. Clear communication about your availability helps foster a smooth remote work experience for you and your team.

## Attendance & PTO Reporting

- Remote employees are expected to follow the same attendance and time-off policies as in-office employees. If you need to take time off, be sure to follow the appropriate request and approval process set by your department. Regular attendance and timely communication about absences help maintain workflow and collaboration.
- For the most up-to-date PTO policies, please contact benefits@lithia.com. If you have any questions about requesting time off, speak with your manager or your HRBP for guidance.

## Labor Law Compliance Posters

- As a remote employee, you are entitled to the same workplace rights and protections as in-office employees. This includes access to federal, state, and company labor law notices, which outline important regulations regarding wages, workplace safety, anti-discrimination policies, and employee benefits.
- Since labor law posters are traditionally displayed in physical workplaces, remote employees must review them digitally. You can access these notices through mandatoryview.com/productview to stay informed about your rights and responsibilities.
- It is important to familiarize yourself with these labor laws, including wage and hour regulations, family and medical leave, workplace safety, and anti-discrimination policies. If you have any questions or concerns about labor laws or your rights as a remote worker, please contact HR or your manager for guidance.


# Technical Support & Troubleshooting

## Report an IT Issue

If you're experiencing a technical problem—like trouble logging in, software errors, or hardware malfunctions, our ServiceNow team is here to help. Common IT issues include:

- Problems accessing systems or applications
- Computer performance issues
- Software bugs or crashes
- Hardware malfunctions (e.g., printers, monitors, keyboards)
- To report an IT issue, submit a request through ServiceNow or contact the IT Help Desk.

Submit a ticket through **Request & Resources** Tile on SPARK or call 1-541-770-2150

## Report a Security Concern

Security concerns involve anything that could put company data or systems at risk. If you notice something suspicious, report it immediately to the **Security Operations Center** by emailing IS-SecurityOperations@lithia.com. Examples include:

- Phishing emails or suspicious links
- Unauthorized access to systems or data
- Lost or stolen company devices
- Unusual activity on your accounts
- Reporting security concerns quickly helps prevent potential threats.

## Report a Risk

Risks are potential vulnerabilities that could impact the company if left unaddressed. These reports go to our **Governance, Risk, and Compliance** (GRC) team for review. Examples include:

- Gaps in security policies or controls
- Compliance concerns with industry regulations
- Vendor or third-party security risks
- Internal process weaknesses that could lead to data exposure
- To report a risk, follow the GRC team's process for submission, or reach out for guidance.

Send an email with your concern to IS-GRC@lithia.com


# Data Protection

## Handling Data at Lithia & Driveway

As a remote employee, you play a vital role in protecting the confidentiality, integrity, and availability of company and customer information. Lithia & Driveway expects all employees to handle sensitive data responsibly and in accordance with internal policies and applicable data privacy laws.

In your role, you might handle **PII (Personally Identifiable Information)** which includes names, addresses, phone numbers, Social Security Numbers, etc. You may also work with **NPI (Nonpublic Personal Information)** which is typically information like financial records, insurance information, and customer transaction details.

This is considered "Sensitive Data" and improper handling of this information can lead to data breaches and legal consequences. For more information, take the training "Handling Data at Lithia & Driveway" or review the Data related policies in the Information Security Policy Portal.

## Best Practices for Data Protection

- **Use Approved Tools:** Store documents only in approved, secure platforms like SharePoint or OneDrive—never on personal drives or USBs.
- **Label Accordingly:** Apply Sensitivity Labels when creating or sharing files to ensure appropriate access and handling.
- **Avoid Printing Sensitive Data:** Only print confidential information if necessary, and store or dispose of it securely.
- **Follow Privacy Laws:** Be aware of and comply with laws like GDPR, CCPA, and PIPEDA, depending on your location or the data you handle.
- **Report Concerns:** If you suspect a data breach or mishandling of sensitive information, report it immediately to IS-SecurityOperations@lithia.com.


# Cybersecurity

Wherever possible, apply the same work practices at home as you would in your normal place of work. Here are some specific examples and guidelines for working at home securely:

## Workspace & Device Security

- Set up a dedicated workspace that is private and secure
- Avoid working in areas where your screen or documents can be easily seen by others.
- If possible, use a screen privacy filter to prevent visual eavesdropping.
- Always lock your computer screen when stepping away from your workstation.
- Use strong, unique passwords and follow our processes for multi-factor authentication (MFA) for all Lithia systems.

## Access & System Security

- Log into Lithia systems at the start of your workday and log out when you are done working.
- Do not share your work device or login credentials with anyone, including family members.
- If you suspect any suspicious activity or security incidents, report them immediately to IS-SecurityOperations@lithia.com.

## Internet & Network Security

- Preserve home internet bandwidth for work activities to maintain efficiency:
  - Reduce the number of non-essential devices connected to your home Wi-Fi
  - Limit the use of streaming services during active working hours (e.g., Hulu, Netflix, Amazon Prime Video).
  - Consider using a separate internet connection (e.g., a mobile hotspot) for personal internet use.
- Improve the performance and security of your home network:
  - If your router is older than 3-5 years, contact your ISP for an upgrade or check for firmware updates.
  - Reboot your router periodically to enhance speed and stability.


  - If your home Wi-Fi router supports 5GHz, use this network for your work computer to reduce interference and improve speed.
  - Enable automatic updates for your router, computers, and other internet-connected devices to ensure the latest security patches are applied.
- Avoid using public or shared Wi-Fi networks unless necessary
  - If you must use public Wi-Fi, connect through the LITHIA VPN to ensure encrypted communication.
- Consider disabling “Wi-Fi Calling” on your cell phone if you have a strong cellular signal, as this may improve your connection stability
- Lithia IT cannot support home networking equipment. If you experience issues, contact your ISP for assistance.

## Document Security

- Minimize the printing of documents; use electronic copies whenever possible.
- If a document must be printed, store it securely (e.g., in a locked drawer).
- Never dispose of sensitive paper documents in regular trash or recycling bins.
- Retain necessary documents securely and return them to the office when possible.
- If documents cannot be returned to the office, securely dispose of them using one of the following methods:
  - Take them to a certified shredding service (e.g., Staples, UPS, or another approved provider).
  - Use a home shredder with cross-cut or micro-cut functionality to ensure secure destruction.
- If handling confidential or sensitive electronic documents
  - Use Lithia-approved encrypted storage solutions
  - Avoid storing work documents on personal devices or cloud services not approved by Lithia IT


# Business Continuity Planning

## Communication Channels

In the event of an emergency, call your direct manager. Personal information should be exchanged ahead of time to ensure information is available during the emergency.

Other channels of communication include:

- Email
- Teams
- Phone (voice and text)
- Video Conferencing (e.g., Microsoft Teams, Webex)

### Emergency Contacts

Your direct manager should be made aware of any emergency contacts and will notify appropriate parties as needed.

## Emergency Scenarios and Procedures

### Natural Disasters

In the event of a natural disaster, such as a hurricane or earthquake, team members should follow these general guidelines:

- Stay informed about local weather and emergency alerts.
- Follow evacuation orders or shelter-in-place recommendations from local authorities.
- Notify the team of your situation and safety as soon as possible.
- If communication is disrupted, try alternative methods such as text messages or social media.
- Use video conferencing if available to visually verify safety.

### Medical Emergencies

In case of a medical emergency, follow these steps:

- Call local emergency services (911 in the United States) if necessary.
- Notify your manager and the team about the situation.
- Share your location and any relevant medical information.
- Follow medical advice and instructions.


### Security Incidents

If you encounter a security incident, such as a break-in or threat, take the following actions:

- Ensure personal safety first.
- Contact local law enforcement if needed.
- Notify your manager and the team about the incident.
- Share any information that can assist in resolving the situation.

## Power Outages

Power outages can occur unexpectedly and may last for extended periods, affecting our ability to work remotely effectively. These procedures and guidelines define how to handle power outages during extended durations to ensure minimal disruption to our remote team's productivity and well-being.

### Power Outage Preparedness

To minimize the impact of power outages, team members are encouraged to take proactive measures:

- **Backup Power Sources:** Consider investing in uninterruptible power supplies (UPS) or portable generators to maintain essential devices (e.g., computer, modem, phone) during power outages.
- **Device Charging:** Keep devices fully charged when not in use to maximize their operational time during an outage.
- **Communication:** Inform your manager and team about your situation when a power outage occurs and your estimated duration of unavailability.

### Temporary Work Locations

During extended power outages, consider the following options for temporarily relocating your workspace:

- **Local Libraries or Cafes:** Identify nearby libraries, cafes, or co-working spaces with power backup or reliable Wi-Fi access.
- **Alternate Residences:** If possible, consider relocating to a friend or family member's residence with power.
- **Company Workspace:** Check if there are any company-owned or affiliated workspaces available for use during outages.


### Communication Protocols

Maintain open communication with your manager and team:

- **Status Updates:** Regularly update your status regarding your availability, estimated duration of the outage, and any potential impact on project timelines.
- **Remote Meetings:** If your internet connection is unstable, communicate this to your team in advance to reschedule or adapt meeting formats.

**Task Prioritization:** During extended power outages, prioritize tasks that can be accomplished offline or with limited connectivity. Coordinate with your manager to adjust project timelines as needed.

**Data Backup:** Regularly back up your work to cloud-based storage or external hard drives to prevent data loss during unexpected outages.

**Flexible Work Hours:** Talk with your manager about accommodating flexible hours due to power outages.

**Reporting Equipment Issues:** If a power outage damages your equipment, promptly report it to your manager or IT support for possible replacement or repair.

**Safety First:** In the event of severe weather or natural disasters causing power outages, prioritize personal safety. Do not attempt to work in unsafe conditions.

## Support & Assistance

Your manager is responsible for providing support and assistance to team members during emergency situations. Please do not hesitate to reach out for help or guidance at any time.

### Local Resources

It is advisable to be aware of local resources and emergency information specific to your region. This can include knowing the location of local hospitals, emergency shelters, and community resources.

### Personal Emergency Kits

Consider maintaining a personal emergency kit at your remote work location. These kits should include essential items such as water, non-perishable food, first aid supplies, flashlights, batteries, and important documents. Be prepared to sustain yourself for at least 72 hours in case of a disaster.

### Reporting Protocol

Report any safety concerns or potential hazards in your remote work environment. By staying proactive, we can address issues before they become emergencies.


# Communication and Collaboration Tools

Staying connected, organized, and secure is key to successful remote work. Lithia & Driveway provides a suite of approved tools to help you communicate effectively, collaborate seamlessly, and protect company information.

## Microsoft Office 365 Platform for Productivity

This is your primary toolkit for daily communication and collaboration. It includes:

- **Outlook** – email and calendar
- **Teams** – chat, video calls, and virtual meetings
- **SharePoint & OneDrive** – secure file sharing and storage
- **Copilot** – AI-powered assistance integrated into apps like Word, Excel, and Outlook to help you draft content, summarize information, and streamline routine tasks

Use these tools first before seeking alternatives—they're secure, supported, and designed to help you work smarter.

## Communications Best Practices

- Be clear and concise in your communications. Use bullet points, headers, and bolding in longer messages.
- Use Teams chat or email for quick updates or clarifications.
- Default to written updates when the message doesn't require a meeting.
- Overcommunicate availability—update your Teams status and let others know when you're heads-down, in meetings, or away.
- Respect boundaries. Be mindful of others' time zones and working hours.

## Best Practices for Information Sharing

- Share files through **Teams**, **SharePoint**, or **OneDrive**, not email attachments when possible.
- Limit access permissions to only those who need it.
- Don't store or send sensitive info through unapproved channels.
- Be sure to encrypt sensitive information by using the tools in Microsoft applications.


# Video Conferencing Best Practices (Teams)

- Join meetings on time and with your audio/video tested.
- Mute yourself when not speaking.
- Use video thoughtfully and professionally.
- Share your screen only when necessary and keep unrelated tabs closed.

**Meeting Etiquette**

- Use an agenda when hosting.
- Stay engaged and avoid multitasking.
- Follow up with clear next steps.
- Respect meeting time—start and end on schedule.

**Department-Specific Tools**

Some teams may use additional approved platforms (e.g., CRM, design, or project management tools).

- Ask your leader which tools your team uses.
- Never download or install unapproved software without IT/InfoSec clearance.

**Use of Personal Communication Apps**

- Do not use personal messaging or email apps (e.g., Gmail, WhatsApp) for company communication.
- All work-related communication must take place in secure, company-approved platforms.

If you have any questions about these directions, please reach out to IS-GRC@lithia.com


# Travel & Expense Policy

## Overview

Managing travel and expenses as a remote employee requires careful planning and adherence to company policies. Whether using a **company credit card**, booking **business travel**, or requesting **reimbursements**, employees must follow established guidelines to ensure compliance and proper expense management.

Additionally, those traveling internationally must take extra precautions to protect company data and maintain secure access to Lithia & Driveway's IT systems.

This section outlines the key policies and procedures remote employees need to know when managing travel and expenses.

## Company Credit Card Policy

Lithia & Driveway provides company credit cards to authorized employees for business-related expenses. Issued through US Bank (Mastercard), these cards remain company property and must only be used for approved purchases like travel and supplies. Remote employees can request a card by emailing creditcards@lithia.com, and cards will be shipped to their home address on file. Cardholders are responsible for activating their card, reviewing training materials, obtaining receipts, and reconciling transactions in **Concur**. For full details, see the **Company Credit Card Policy** on **DocXplorer**, or contact creditcards@lithia.com with questions.

## Travel & Expense Policy

Remote employees may occasionally need to travel for business purposes. Lithia & Driveway's Employee Travel & Expense Policy ensures consistency and compliance when incurring work-related expenses.

### Key Points for Remote Employees:

- **Travel Authorization:** All business travel must be pre-approved by your leader before booking.
- **Booking Travel:** Use Concur to book flights, hotels, and rental cars. Advance booking (14+ days) is encouraged to optimize cost savings.
- **Expense Reimbursement:** Employees should submit expenses through Concur with proper documentation. Reimbursements are processed within 3-5 business days after approval.


- **Company Credit Card Usage:** If you have a corporate credit card, use it for business expenses only. Personal expenses on company cards are prohibited.
- **Meal Allowance:** A daily per diem applies to business travel days ($50/day or $70/day for specific locations).
- **Transportation & Lodging:** Economy-class airfare, standard hotel rooms, and intermediate-size rental cars are the default choices unless pre-approved for upgrades.
- **Personal Car Use:** Employees using personal vehicles for business travel are reimbursed at the current mileage rate but must exclude daily commuting mileage.
- **Non-Reimbursable Expenses:** Items such as personal entertainment, alcohol (unless pre-approved), traffic fines, and loyalty program fees are not eligible for reimbursement.

For more details, including detailed reimbursement guidelines and corporate credit card policies, please refer to the **Employee Travel & Expense Policy** on **DocXplorer**. If you have any questions, contact creditcards@lithia.com or reach out to TSI Travel Support at 800-642-7547.

## Travel Exceptions

Employees traveling outside the U.S. who need access to **Lithia & Driveway's IT infrastructure** must follow the **International (Transitory) Travel Policy** to ensure security and compliance. Employees must notify IS-SecurityOperations@lithia.com at least **10 business days before departure** and obtain manager approval for temporary access. While abroad, employees are required to use **VPN at all times**, avoid **public Wi-Fi**, and comply with **local laws** on encryption and remote access.

Access from certain **restricted countries** is prohibited unless explicitly approved for business purposes. Employees must also adhere to **data privacy regulations** (e.g., GDPR) and protect company assets. IT access will be **revoked upon return** or if security policies are violated. For full details, see the International Travel Policy in **the Information Security Policy Portal** or contact IS-SecurityOperations@lithia.com with questions.


# Work-From-Home *Best Practices*

1. **Establish a Routine**
    - Start and end your day at the same time to maintain consistency.
    - Get dressed as if you were going to the office to shift into a work mindset.
    - Schedule breaks to avoid burnout and refresh your focus.

2. **Create a Dedicated Workspace**
    - Set up a quiet, organized, and comfortable workspace.
    - Ensure proper ergonomics to prevent strain or discomfort.
    - Keep work-related items separate from personal belongings.

3. **Maintain Clear Communication**
    - Use company-approved communication tools (e.g., email, chat, video calls).
    - Set expectations for response times and availability with your team.
    - Participate actively in virtual meetings and discussions.

4. **Stay Secure & Protect Company Data**
    - Use a **VPN** when accessing company systems.
    - Lock your screen when away from your workstation.
    - Follow **data security policies** (e.g., avoid saving sensitive info on personal devices).
    - Report any **phishing attempts or security concerns** to IT.

5. **Manage Productivity & Time Effectively**
    - Set daily goals and prioritize tasks.
    - Use productivity tools (e.g., task lists, calendars, project management software).
    - Minimize distractions (turn off social media, use noise-canceling headphones).

6. **Stay Connected with Colleagues**
    - Check in regularly with your team to stay engaged.


- Participate in virtual team-building activities.
- Be proactive in asking for feedback and offering support.

7. **Balance Work & Personal Life**
    - Set clear boundaries between work and home life.
    - Take scheduled breaks, including lunch, away from your desk.
    - Avoid working beyond scheduled hours to prevent burnout.

8. **Take Care of Your Well-Being**
    - Stretch and move throughout the day.
    - Maintain a healthy diet and stay hydrated.
    - Get sufficient sleep and manage stress effectively.

9. **Ensure Reliable Technology**
    - Keep your software and system updates current.
    - Have backup solutions for internet or power outages.
    - Contact IT support promptly for technical issues.


# Reporting Issues & Concerns

Even while working remotely, it's important to speak up when something goes wrong. Lithia & Driveway provides clear channels for reporting technical issues, security concerns, HR-related matters, and work-related injuries. Prompt reporting helps us respond quickly and ensure the safety, security, and well-being of all employees.

## IT Issues or Security Breaches

If you experience technical problems, need assistance with software, or suspect a potential **cybersecurity threat** (such as phishing, unauthorized access, or data loss), submit a ticket through the **Lithia & Driveway Request & Resource Center (ServiceNow)** or call the **IT Help Desk**:

- **US:** +1 541 770 2150
- **Canada:** 877 309 0908
- For security incidents, you can also contact IS-SecurityOperations@lithia.com directly.

## HR-Related Concerns

For questions about **workplace behavior**, **employee relations**, or **policies**, contact your HR Business Partner (HRBP) or Employee Relations at employeerelations@lithia.com. You can find your HRBP in the Store Roster on DocXplorer or ask your manager.

For benefits or Total Rewards questions, review the **Total Rewards Guide** or email benefits@lithia.com. You can also view and manage your benefits in **Workday.**

To report sensitive matters confidentially, visit the **Ethics Hotline** via SPARK under Employee Resources.

## Reporting Work-Related Injuries While Remote

In the event of an injury that occurs while working from home during work hours, notify your **manager** immediately and file a report with **Employee Relations**. Be prepared to provide details such as the time, location, and nature of the injury. Remote employees are covered under the same workplace injury policies as on-site staff, and timely reporting is essential for proper documentation and support.

If you're ever unsure where to report something, your manager or HRBP can help guide you to the right place.