DiamondRock Hospitality Company

Cybersecurity Policy

DiamondRock Hospitality Company's ("DiamondRock" or "Company") cybersecurity policy outlines our guidelines and readiness for preserving the security of our data, managing communications, and training and protecting our technology infrastructure.

DiamondRock 's strategy relies on technology and cloud-based software products for collecting, storing and managing critical and private information and thus our vulnerability to security breaches and other cybersecurity threats is constant and ever-present. Threats to the Company's financials, non-public information, and reputation include malicious malware, hackers, human errors and system malfunctions.

To counterbalance these concerns, we have implemented several security and training measures which are outlined below. This policy also identifies key cybersecurity risks. This policy applies to all Company employees, contractors and anyone who has permanent or temporary access to our systems and hardware.

Maintaining Confidentiality

Confidential data is secret and valuable. Confidential data includes, but is not limited to:

- Undisclosed financial information
- Undisclosed operational and investment information
- Data of customers/partners/vendors
- Bank account and routing information
- Payroll data for employees

DiamondRock corporate employees are required to safeguard and protect this data. The risk and mitigation guidelines below provide instructions on how to prevent security breaches.

Protect Personal and Company Devices

When employees use their digital devices, whether on office, home or public networks, to access Company emails, the network, or internet accounts, security risks are introduced to our systems and confidential data. We advise our employees to keep both their personal and company-issued computer, tablet, cell phone and any other electronic devices secure. In order to minimize risk, employees must aim to complete the following on Company issued devices and any personal device used to access Company data:

- Keep all devices password protected.
- Complete necessary security system updates and patches.
- For home networks, ensure updated antivirus software.
- Ensure devices are not exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.
- VPN is only permitted on company issued computers.
- Use secure VPN or Citrix when accessing company network or company data.

We advise employees to avoid accessing internal systems and accounts from other people's devices or lending devices with access to our systems or accounts to others.

When employees (existing or new) receive company-issued equipment, they receive instructions for:

- RSA Token and password management setup including mandatory dual factor authentication setup
- Microsoft software setup

- Setting up and accessing Citrix and VPN network

Keep Emails Safe

There are two key types of malicious emails for employees to be on alert for: 1) spoofing an internal or external email address, and 2) external contacts that have been infected and are sending out infected emails. To avoid virus infection or data theft, we instruct employees to:

- Check email addresses and names of people sending the message to ensure legitimacy.
  - Is the email address the correct address? Does the subject line make sense? Were you expecting this email? Did this email arrive at the expected time?
- Avoid opening attachments; hover over hyperlinks to see if the website address aligns with the sender and the message.
- Avoid clicking on links when the content is not adequately explained, or the email has no additional information.
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Before completing any actions, evaluate the email for any inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- Avoid emails requesting any type of banking information or money transfer. Follow established protocols for money related transactions.
- Confidential data is not permitted to be sent to employees' personal email accounts.
- Notify IT of any spam emails to add to the blocked list of addresses within the mail filter.
- Manage your daily mail filter system to ensure cleared emails are not being blocked in the filter.
- When in doubt about the legitimacy of an email, please forward to the IT department for their review.

The Company intermittently sends "suspicious" emails to employees in order to test compliance with email policies and to educate employees on prevention of future breaches.

Manage Passwords Properly

Compromised passwords are dangerous as they can harm or infect our entire infrastructure. While computer and outlook mail access rely on two-factor authentication currently provided thru RSA or Microsoft, our network and systems are still at risk given that many applications and websites used on our network only require passwords. Network and confidential system passwords should be secure and kept secret. For this reason, we require our employees to do the following:

- DiamondRock system passwords must be at least [**fourteen] characters** and must include capital and lower-case letters, numbers, and symbols. Employees are encouraged to avoid information that can be easily guessed (e.g. birthdays.)
- Change passwords every 90 days unless protocol is adjusted by the IT department due to business needs.

IT Notification

Our IT department needs to know about scams, breaches, spam emails that make it through our mail filters, and malware so they can better protect our infrastructure. For this reason, we require all employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to the IT team. The IT department will investigate promptly, resolve the issue and send a companywide alert when necessary.

Our IT team is responsible for training and advising employees on how to detect scam emails and we encourage our employees to reach out to them with any questions or concerns.

Additional Measures

We also provide employees with the following guidelines as additional recommended security measures:

- Report stolen or damaged equipment as soon as possible to IT.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on Company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our Social Networking Policy and Code of Business Conduct and Ethics.

Our IT Department will:

- Install and continuously monitor for upgrades and improved software for firewalls, anti-malware software, mail filters and access authentication systems.
- Conduct cybersecurity and email training sessions for all employees on an on-going basis.
- Provide information regularly to employees about new scam emails or viruses and ways to combat them.
- Monitor employee access rights to systems and secured folders on the company network.
- Investigate security breaches thoroughly.
- Conduct a third-party security test annually.
- Evaluate other types of mail and access testing systems for deploying as employee training purposes.
- Follow all cybersecurity policies.
- If business needs change, address any adjustments or modifications to the protocols in this list with the Chief Financial Officer.

Remote Employees

This policy applies to all full-time and part-time employees, including those working remotely. Remote employees are obligated to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage all employees that work while outside of the corporate office to consult with the IT department on network security.

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face the following disciplinary action:

- Unintentional and small-scale security breach: we may issue a verbal and / or a written warning and train the employee on security.
- Intentional, repeated or large-scale breaches (which cause severe financial or other damage): we will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by-case basis.

Take Security Seriously

All employees must take cybersecurity seriously at all times. Employees need to remain vigilant and active in the prevention of cyber breaches.