



VENDOR MANAGEMENT

Jon Bonham CISA, QSA
Principal, Coalfire Systems, Inc.

1

AGENDA

About Linda
About Jon and Coalfire

- Requirements 12.8 and 12.9
- Requirement 12.8.5 Responsibility Matrix
- Requirement 12.8.1 List of Service Providers
- Requirement 12.8.2 Written Agreements
- Requirement 12.9 Written Agreements
- Requirement 12.8.3 Hiring Service Providers
- Requirement 12.8.4 Monitor Service Providers



2

If you have a question, shout it out.



COALFIRE

3

JON BONHAM

Been with Coalfire for over 10 years.

Works with Universities, State and local governments and hospital systems.

Live in TN with my wife. 3 kids all grown and living around the world.

Coalfire has been around since 2001. Currently has about 700 employees.

PCI is the largest practice but also does HIPAA, FISMA, FEDRAMP, CLOUD, Scans, Pen-testing and most other areas including GDPR



COALFIRE

4

WHY WE ARE HERE

Requirement 12.8 and 12.9

C CAL FIRE

5

REQUIREMENT 12.8.5

Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity? (12.8.5)



C CAL FIRE

6

REQUIREMENT 12.8.1

Is a list of service providers maintained? (12.8.1)



CAL FIRE

7

Requirement 12.8.1

The image shows a comprehensive checklist for 'VAN HALEN DRESSING ROOMS'. It is organized into several sections:

- Left Column:** 'VAN HALEN Presents The World's Most Demanding Concert Rider'. It lists 'DINNER - SAND + ONE (5 PEOPLE)', 'Cold Drinks' (with quantities like 1.5, 1, 2, 1, 1, 1, 1, 1, 1, 1), and 'Room Temperature Drinks' (with quantities like 2, 3, 1, 2, 2, 1).
- Middle Column:** 'DRESSING ROOMS' floor plan showing room layouts. Key rooms include:
 - BAND HOSPITALITY ROOM:** 2 large tables, 200 chairs, 4 propane heaters.
 - BAND ROOM:** 1 large table, 10 chairs, 1000 chairs, 1000 chairs.
 - CHANGING ROOM:** 1 lock to be removed, 1000 chairs, 1000 chairs.
 - TURNOFF ROOM:** 1 outdoor table, 1000 chairs, 1000 chairs, 1000 chairs.
 - CREW ROOM:** 1 large table, 1000 chairs, 1000 chairs, 1000 chairs.
- Right Column (Trays and Supplies):**
 - Deli Tray:** Includes items like bread, butter, jam, and various meats.
 - Cheese Tray:** Includes items like cheese, crackers, and dips.
 - Vegetables:** Includes items like tomatoes, cucumbers, and carrots.
 - Fruit:** Includes items like apples, oranges, and grapes.
 - Hot Drinks:** Includes items like coffee, tea, and hot chocolate.
 - Supplies:** Includes items like plates, cups, napkins, and cleaning supplies.

At the bottom, it states: 'ALL ROOMS MUST BE LOCKABLE AND KEYS GIVEN TO THE TOUR MANAGER, STAGE MANAGER, AND SECURITY DIRECTOR.'

CAL FIRE

8

REQUIREMENT 12.8.2

Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? (12.8.2)

NOTE: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.

CAL FIRE

9

REQUIREMENT 12.9

Do service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? (12.9)



CAL FIRE

10

REQUIREMENT 12.8.3

Is there an established process for engaging service providers, including proper due diligence prior to engagement? (12.8.3)

CALFIRE

11

REQUIREMENT 12.8.4

Is a program maintained to monitor service providers' PCI DSS compliance status at least annually? (12.8.4)



CALFIRE

12

WHAT ELSE IS THERE FOR E-COMMERCE?

PCI-DSS 1.2

Anything that STORES, PROCESSES or TRANSMITS payment card data.

V3.0

Is connected to or...

CALFIRE

13

WHAT ELSE IS THERE FOR E-COMMERCE?

PCI-DSS 1.2

Anything that STORES, PROCESSES or TRANSMITS payment card data.

V3.0

Is connected to or...

Can impact the security of.

CALFIRE

14

Questions



JON BONHAM CISA, QSA
PRINCIPAL
Coalfire Systems, Inc.
Cyber Assurance Services
jbonham@coalfire.com

C  A L F I R E