COALFIRE

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**

COALFIRE

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

COALFIRE

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)

COALFIRE

6

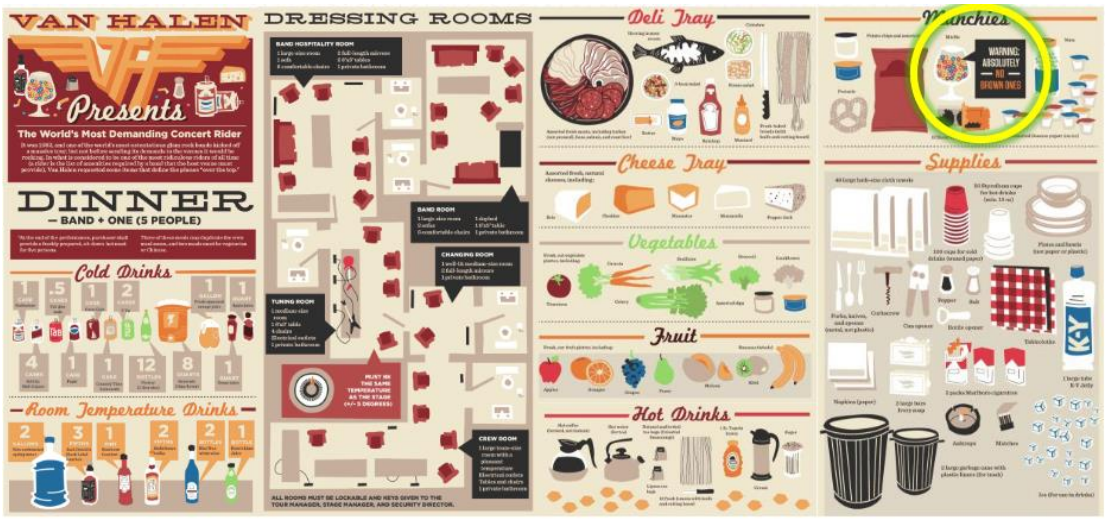
REQUIREMENT 12.8.1

Is a list of service providers maintained? (12.8.1)

CALFIRE

7

Requirement 12.8.1



CALFIRE

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.

COALFIRE

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)

COALFIRE

10

REQUIREMENT 12.8.3

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

COALFIRE

11

REQUIREMENT 12.8.4

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

COALFIRE

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…

COALFIRE

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.

COALFIRE

14

Questions

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

COALFIRE

15