INFORMATION SECURITY BASELINE REVIEW

January 31, 2016

Prepared for:
Graceland, Inc.

Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

January 31, 2016

Elvis Presley
Sr. Director of Rock and Roll
Graceland, Inc.
3000 Graceland Ave.
Memphis, Tennessee

Dear Elvis:

Thank you for allowing us the opportunity to offer our services to the Graceland, Inc. Attached you will find a report on the results of our Information Security Baseline Review, as outlined in our initial proposal.

Our report is the result of interviews with key Graceland, Inc. representatives. The information gathered from these activities was analyzed using ISO Standard 27002-2013 as a basis to identify information security risks and aid in the development of recommendations. Categories addressed in our report include, but are not limited to: Information Classification, Third Party Service Delivery Management, Exchange of Information, Monitoring and Compliance.

You will find a focus chart that provides a high-level view of your current information security landscape in addition to individual category charts to assist you in identifying the areas of greatest concern to the Organization. We have also developed recommendations to aid the Graceland, Inc. on your path to security. The recommendations contained in this report are not comprehensive and are intended for review purposes, in addition to the continued development of IT security policies and procedures.

Very truly yours,
Dopkins & Company, LLP
by:

William M. Prohn
Managing Director

Table of Contents

1 Letter

2 Self Assessment

3 Focus Chart

4 Topics

Information Security Policies

Organization of Information Security

5 Recommendations

6 Appendix - Best Practices

Self Assessment

The maturity model used in our Information Security Baseline Review is based on COBIT 5 by ISACA. Maturity modelling for management and control over Information Security processes is based on a method of evaluating the organization, so it can be rated from a maturity level of incomplete (0) to optimized (5).

The advantage of a maturity model approach is that it is relatively easy for management to place itself on the scale and appreciate what is involved if improved performance is needed. The scale includes 0 because it is quite possible that no process exists at all. The 0-5 scale is based on a simple maturity scale showing how a process evolves from an incomplete capability to an optimized capability.

An impact scale is used to estimate the impact on the organization if a specific topic was not in place. High represents a catastrophic result affecting mission-critical activities. A medium impact may cause considerable business disruption and would likely affect internal and external parties. A low impact would be a nuisance.

Maturity Model from COBIT 5 by ISACA

5 Optimized—Continuously improved to meet relevant current and projected enterprise goals.

4 Predictable—Operates within defined limits to achieve its process outcomes.

3 Established—Implemented using a defined process that is capable of achieving its process outcomes.

2 Managed—Implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.

1 Performed—Process achieves its process purpose.

0 Incomplete—Not implemented or little or no evidence of any systematic achievement of the process purpose.

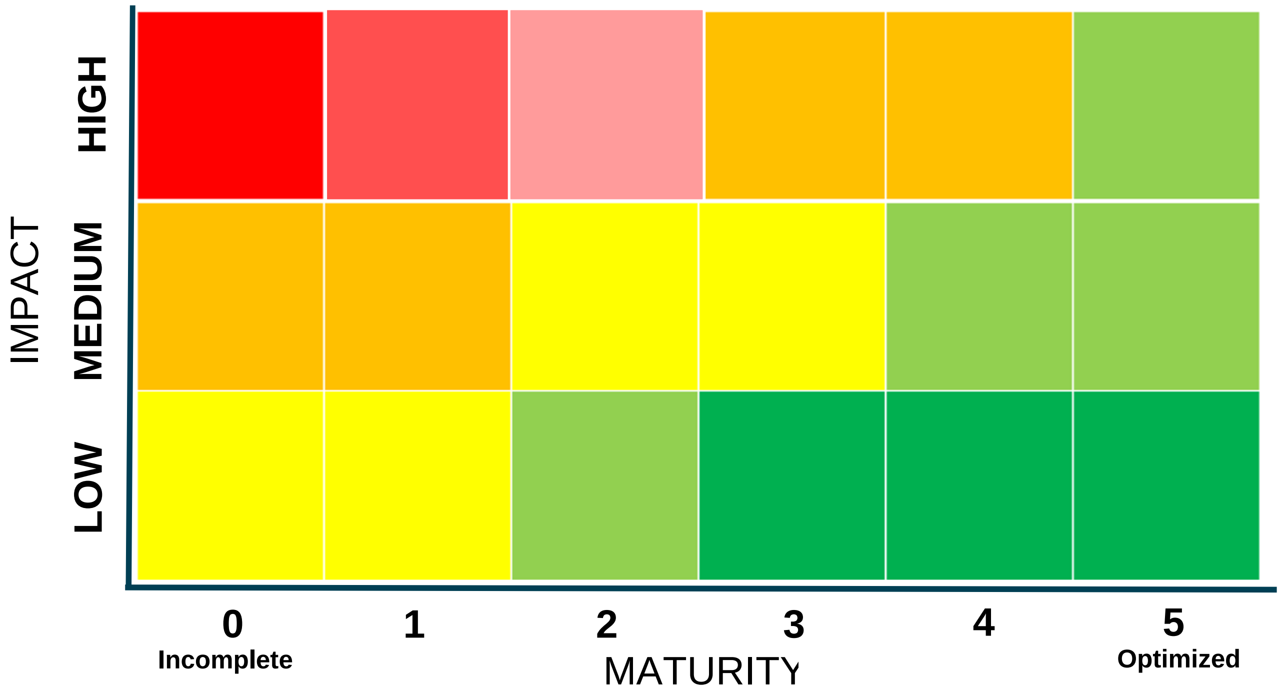
Impact Scale

High—The result could be catastrophic. Mission-critical activities would be impacted. Day-to-day operations of your business would be severely disrupted.

Medium—Mission-critical activities would be impacted and could cause a considerable business disruption. Internal and external parties would be impacted.

Low—The result would be a nuisance. All mission-critical activities would remain operational.

Heat Map



Information Security Checklist based on ISO and NIST Standards

N/A | 0 Incomplete | 1 Performed | 2 Managed | 3 Established | 4 Predictable | 5 Optimized

Information security policies

1	**Policies for information security**	A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.	**N/A 0 1 2 3 4 5**	**2**	**H M L**	**H**
2	**Review of the policies for information security**	The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	**N/A 0 1 2 3 4 5**	**2**	**H M L**	**H**

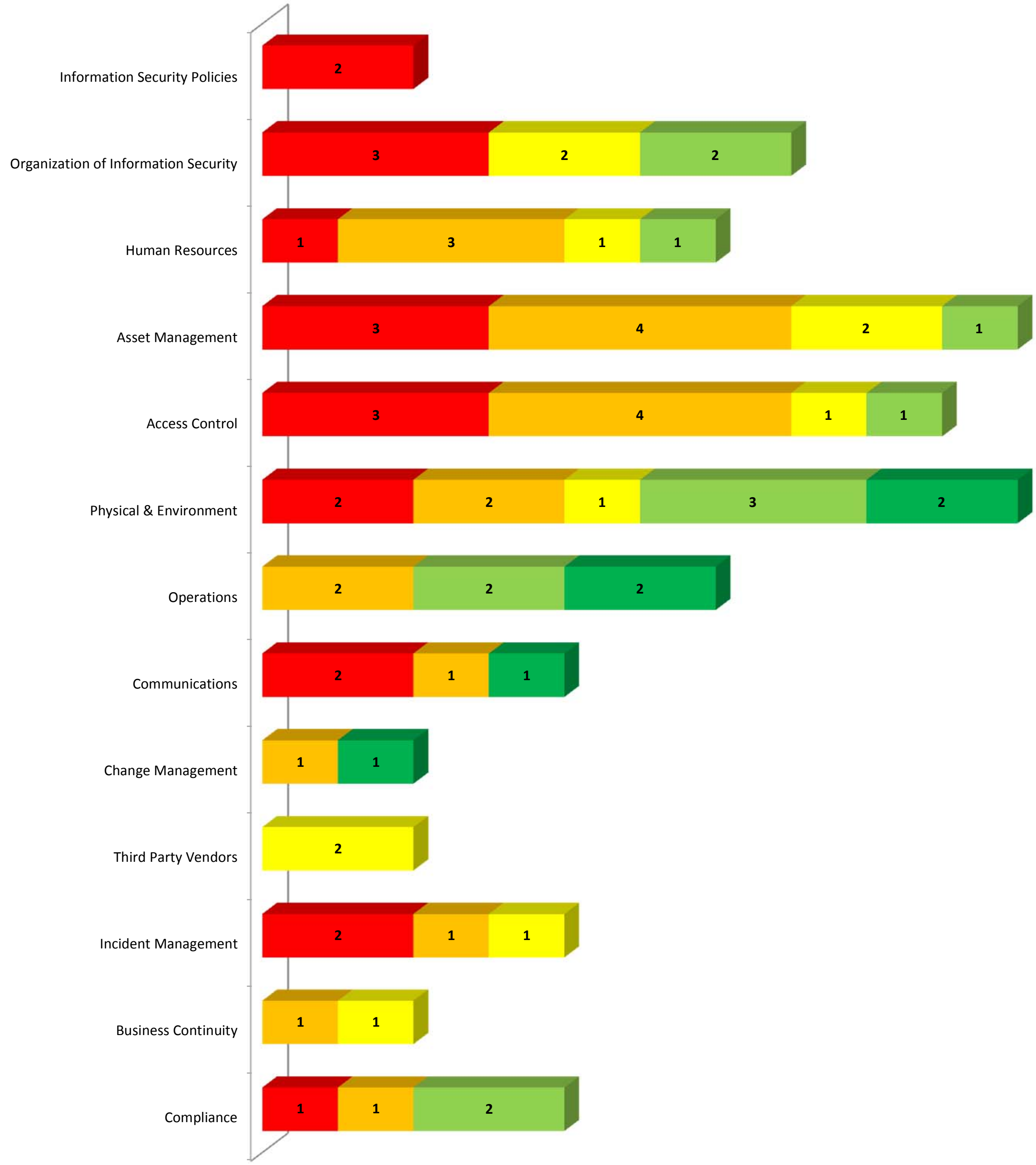
Organization of information security

3	**Information security roles and responsibilities**	All information security responsibilities should be defined and allocated.	**N/A 0 1 2 3 4 5**	**2**	**H M L**	**M**
4	**Segregation of duties**	Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	**N/A 0 1 2 3 4 5**	**2**	**H M L**	**M**
5	**Contact with authorities**	Appropriate contacts with relevant authorities should be maintained.	**N/A 0 1 2 3 4 5**	**2**	**H M L**	**L**
6	**Contact with special interest groups**	Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.	**N/A 0 1 2 3 4 5**	**5**	**H M L**	**M**
7	**Information security in project management**	Information security should be addressed in project management, regardless of the type of the project.	**N/A 0 1 2 3 4 5**	**2**	**H M L**	**H**
8	**Mobile device policy**	A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.	**N/A 0 1 2 3 4 5**	**1**	**H M L**	**H**
9	**Teleworking**	A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.	**N/A 0 1 2 3 4 5**	**1**	**H M L**	**H**

Focus Chart

The Focus Chart illustrates the scores that the Graceland, Inc. has assigned to each topic. The color of each segment was developed using the Heat Map represented in the previous section. Each segment displays the number of topics that fell into that color category.

Focus Chart


Information Security Policies
2
Organization of Information Security
3
2
2
Human Resources
1
3
1
1
Asset Management
3
4
2
1
Access Control
3
4
1
1
Physical & Environment
2
2
1
3
2
Operations
2
2
2
Communications
2
1
1
Change Management
1
1
Third Party Vendors
2
Incident Management
2
1
1
Business Continuity
1
1
Compliance
1
1
2

Topics

Each topic page contains a graph illustrating the scores that the Graceland, Inc. has assigned to each topic. The color of each segment was developed using the Heat Map. Each segment displays the number of topics that fell into that color category.

The topic descriptions are provided below the graph and are listed in order from most to least critical based on the Heat Map. Topics that were deemed N/A have been removed from the list.

Information Security Policies

2

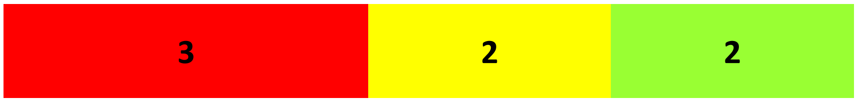
Policies for information security

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Review of the policies for information security

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Organization of Information Security



🟥	**Teleworking**	A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.
🟥	**Mobile device policy**	A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.
🟥	**Information security in project management**	Information security should be addressed in project management, regardless of the type of the project.
🟨	**Information security roles and responsibilities**	All information security responsibilities should be defined and allocated.
🟨	**Segregation of duties**	Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
🟩	**Contact with special interest groups**	Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.
🟩	**Contact with authorities**	Appropriate contacts with relevant authorities should be maintained.

Recommendations

The following recommendations were developed by Dopkins & Company, LLP to address specific areas of concern identified during our Information Security Baseline Review. They are intended to aid in the implementation of information security policies and procedures and should not be considered comprehensive or exhaustive.

Recommendations

1 = Critical 2 = Essential 3 = Important

1 Review & Monitor Administrators' Logs

Logs of administrative activity should be reviewed for appropriateness by an individual other than the system administrator.

We do not recommend maintaining a generic "ADMIN" account. Instead, users should be granted administrative access so that audit logging can effectively identify activity based on the current user. Generic User IDs (i.e. "TEST") should be removed to reduce the likelihood of anonymous activity.

1 Restrict Third Party Vendor's Administrative Access

Your third party vendor should be required to request administrative privileged access on a case-by-case basis (i.e. user ID is inactivated when not in use) and should not retain it 24/7. Third party user ID's used should be identified as such, for example: "Admin-3." Access should be logged after it has been approved.

Third party vendor should inform you when a member of their team leaves or transfers jobs so that Graceland, Inc. can change the administrative password, and should be notified of any breach or information security event at the third party vendor.

1 Develop an End-user Information Security Policy

Develop a comprehensive information security policy for end-users such as employees, interns and vendors. The policy should include specific guidance (do's and don'ts) for employees and interns.

Example topics from a sample end-user policy include:

- Access Control
- Information Classification
- Physical & Environmental Security
- Acceptable Use of Assets
- Clear Desk/Screen
- Appropriate Transfer of Information
- Mobile Devices & Teleworking
- Restrictions on Software and Installation

A comprehensive, reviewed information security policy is a primary requirement of virtually every security standard and legislative regulation (i.e. HIPAA, PCI-DSS, etc.).

Appendix - Best Practices

This appendix contains best practices based on international standards for the topics that you determined were of a high priority to the Graceland, Inc. This guidance is intended to aide in the implementation of information security policies and procedures.

Appendix - Best Practices

Topic: Policies for information security
Recommendation:

Develop a comprehensive Information Security policy to accompany the existing Confidentiality and Technology policies.

The policy should contain statements concerning:

- the definition of information security
- the assignment of general and specific responsibilities and roles for information security
- processes for handling deviations and exceptions
- specific guidance (do's and don'ts) for employees

Example topics from a sample policy include:

- Access Control
- Information Classification
- Physical & Environmental Security
- Acceptable Use of Assets
- Clear Desk/Screen
- Appropriate Transfer of Information
- Mobile Devices & Teleworking
- Restrictions on Software and Installation
- Backup
- Protection from Malware
- Encryption
- Communications Security
- Privacy and Protection of Personally Identifiable Information (PII)

Employees should be required to sign an agreement annually stating that they have read and understood the policy.

Topic: Review of the policies for information security
Recommendation:

Each policy should have an owner who is responsible for the development, review and evaluation of the policy. The review should include assessing opportunities for improvement of the Organization's approach to managing Information Security. Changes to the security environment, business circumstances, legal conditions and the technical environment of the Organization should be taken in to account.

Examples of conditions that may require a modification to the policy include:

- Purchase/implementation of new hardware or software
- The proliferation of a new social media platform
- Updates to NYS guidance on the protection of personally identifiable information
- Development of new positions within the Organization