

October 19, 2005

# Security Analysis

---

## ***Oracle Critical Patch Update – October 2005 Oracle E-Business Suite Impact***

### Overview

Oracle Corporation released the fourth Critical Patch Update (CPU) on October 18, 2005. The CPU is a collection of security related patches for the Oracle Database, Oracle Application Server, Oracle Collaboration Suite, Oracle E-Business Suite and PeopleSoft Applications. There are more than 80 vulnerabilities addressed in the CPU ranging from buffer overflows to SQL injection to denial of service (DoS) issues. Most of the vulnerabilities are high risk and should be addressed quickly.

This analysis provides additional information on the vulnerabilities and patches released in the CPU as they relate to the Oracle E-Business Suite (Oracle Applications 11i). The objective of this analysis is to assist IT managers and database administrators in assessing the impact on their Oracle Applications 11i implementations and the risks associated with the vulnerabilities, especially since the CPU addresses a large number of vulnerabilities and impacts all layers of the Oracle Applications technology stack.

#### **Critical Patch Update Overview**

Oracle has continued the progress started with the last Critical Patch Update (July 2005) of improving the overall security of the Oracle E-Business Suite. A number of the patches included in this and the previous CPU do not necessarily fix security vulnerabilities, but rather cleanup and rectify security issues inherent in Oracle Applications. We are pleased with the progress Oracle is making toward a fundamentally more secure application, however, there is still considerable work to be done.

Even though the CPU does fix over 80 security vulnerabilities, there is a large queue of yet unpatched security bugs. There are more than 100 open security bugs found by independent security researchers in all layers of the technology stack and many of these bugs are deemed high risk. Also, there are reports that some of the security bugs identified as fixed by Oracle in this and previous CPUs, are still exploitable due to errors in the patches or because Oracle implemented inadequate fixes.

Customers should not rely solely on these patches to provide for a secure environment. In addition to promptly applying security patches, the operating system, database, application servers, and application should be “hardened” using Integrigy’s recommendations published by Oracle in the whitepaper “Best Practices for Securing Oracle E-Business Suite” (Metalink Note 189367.1). “Defense in depth” should be employed to protect the database and application servers. Direct connections to the database using SQL\*Net should be limited to the data center and an intrusion detection or prevention solution should be deployed to detect and/or block potential attacks.

### Forced Upgrades

As with the previous CPUs, Oracle is forcing technology stack upgrades on customers. The only significant upgrade in this CPU is to Oracle Applications DBA AD.I.x, as the required versions for the Database, Application Server, Developer 6i, and JInitiator remain the same as the July 2005 CPU. AD.I.x does require implementation of AutoConfig, which is a significant undertaking.

For customers who have not applied patches from previous CPUs, significant upgrades to the technology stack may be required in order to apply many of the security patches. Under some circumstances, upgrading to 11.5.10 CU2 may be less disruptive than individually applying all the required technology stack upgrades.

## Assessment of Vulnerabilities

With information released by Oracle and security researchers and since most of the vulnerabilities are similar in nature to previous vulnerabilities, we believe usable exploits can be easily developed for many of the vulnerabilities in a matter of hours.

### Oracle Database Vulnerabilities (DB01 – DB29)

Many of the database vulnerabilities can easily be exploited using a direct SQL\*Net connection to the database or indirect connection (e.g., reporting tools) that allows a user to execute arbitrary SQL statements. This is especially a problem with Oracle Applications, unless specifically blocked, given that anyone can access the database and logon using the APPLSYSUB account; the APPLSYSUB database account has a well known password and can not be disabled. A number of these vulnerabilities can be exploited using the APPLSYSUB database account, since APPLSYSUB has access to some of the vulnerable database packages by default.

In addition, almost all these vulnerabilities can be exploited via SQL injection vulnerabilities in Oracle Applications. Attacks on the database server can be made using a web browser, even though the attacker does not have direct access to the database server. This possibility will have the greatest impact on those implementations where Oracle Applications web servers are directly connected to the Internet.

### Oracle Application Server Vulnerabilities (AS01 – AS14)

The Application Server vulnerabilities are in various components of the Application Server including the Oracle HTTP Server (Apache), Web Cache, Internet Directory, Oracle Reports, etc. The most relevant issues for Oracle E-Business Suite implementations are the Oracle HTTP Server issues (**AS03** to **AS05**). There are no new Oracle Forms or Oracle Reports vulnerabilities relevant to Oracle Applications fixed in this CPU.

## Oracle E-Business Suite Vulnerabilities (APPS01 – APPS21)

The vulnerabilities in the CPU are a mixture of fixes for security vulnerabilities and a number of patches aimed at resolving inherent security weaknesses in the Oracle Applications. As an example, **APPS12** and **APPS13** are issues with excessive or obsolete system privileges assigned to standard Oracle Applications database accounts, which are not necessarily exploitable unless the default passwords for these database accounts have not been changed. Another example is **APPS02**, which relates to the standard 18 Oracle Applications default application accounts that are enabled and have default passwords when Oracle Applications is installed.

The other vulnerabilities range everywhere from permission issues in HR Self-Service to SQL injection in workflow database packages to denial of service issues. Overall, a number of these vulnerabilities should be considered high risk and corrected immediately.

## Patch Analysis

For the Oracle E-Business Suite, install the patches as specified in "Note 333963.1 Oracle Critical Patch Update October 2005 Pre-Installation Note for Oracle E-Business Suite" and you should also review the Pre-Installation Notes for the Oracle Database and Oracle Application Server prior to installing those patches.

### Technology Stack Upgrades

With the release of each CPU, Oracle has required some upgrades to the technology stack by supporting only recent patchsets for the Database, Application Server, Developer 6i, JInitiator, and Applications Object Library (AOL). These required technology stack upgrades have delayed many organizations in applying the patches in the CPU due to the added complexity and time required to apply the security patches as well as the technology stack upgrades. For some organizations, the required technology stack upgrades can be significant and may even necessitate a migration to AutoConfig.

### 1. All Previous CPUs Applied – Required Technology Stack Upgrades

If you have already applied the patches from the July 2005 CPU and prior CPUs, the only significant technology stack upgrade required to Oracle Application DBA (AD) Minipack I.1 or I.2 (AD.I.1 was released March 31, 2005 and AD.I.2 was released July 27, 2005). The required patch levels for the Database, Application Server, Developer 6i, and JInitiator all remain the same as the July 2005 CPU.

**2. All Previous CPUs NOT Applied – Required Technology Stack Upgrades**

The following table shows the supported patchsets (black) and unsupported patchsets (red italics) for the October 2005 CPU –

	Database	Application Server	Developer	JInitiator (WinXP)	Applications (base FND.x)
11.5.1	<i>8.1.6</i> <i>8.1.7.1</i> <i>8.1.7.2</i> <i>8.1.7.3</i> 8.1.7.4	<i>1.0.2.1.x*</i> 1.0.2.2.2	<i>6.0.8.8.0</i> <i>6.0.8.x (P1 – P15)</i> 6.0.8.25 (P16)	<i>1.1.7.27</i> <i>1.1.8.16 – 22</i> <i>1.3.1.9</i> <i>1.3.1.14</i>	<i>FND A – C</i> FND.D – H
11.5.2	<i>8.1.6</i> <i>8.1.7.1</i> <i>8.1.7.2</i> <i>8.1.7.3</i> 8.1.7.4	<i>1.0.2.1.x*</i> 1.0.2.2.2	<i>6.0.8.8.0</i> <i>6.0.8.x (P1 – P15)</i> 6.0.8.25 (P16) 6.0.8.26 (P17)	<i>1.1.7.27</i> <i>1.1.8.16 – 22</i> <i>1.3.1.9 - 17</i> 1.3.1.21	<i>FND B – C</i> FND.D – H
11.5.3	<i>8.1.6</i> <i>8.1.7.1</i> <i>8.1.7.2</i> <i>8.1.7.3</i> 8.1.7.4	<i>1.0.2.1.x*</i> 1.0.2.2.2	<i>6.0.8.8.0</i> <i>6.0.8.x (P1 – P15)</i> 6.0.8.25 (P16) 6.0.8.26 (P17)	<i>1.1.7.27</i> <i>1.1.8.16 – 24</i> <i>1.3.1.9 - 18</i> 1.3.1.21	<i>FND C</i> FND.D – H
11.5.4	<i>8.1.6</i> <i>8.1.7.1</i> <i>8.1.7.2</i> <i>8.1.7.3</i> 8.1.7.4	<i>1.0.2.1.x*</i> 1.0.2.2.2	<i>6.0.8.8.x</i> <i>6.0.8.12.1 (P3)</i> <i>6.0.8.x (P1 – P15)</i> 6.0.8.25 (P16) 6.0.8.26 (P17)	<i>1.1.8.7</i> <i>1.1.8.16 – 24</i> <i>1.3.1.9 - 18</i> 1.3.1.21	<i>FND.C</i> FND.D - H
11.5.5	<i>8.1.6</i> <i>8.1.7.1</i> <i>8.1.7.2</i> <i>8.1.7.3</i> 8.1.7.4	<i>1.0.2.1.x*</i> 1.0.2.2.2	<i>6.0.8.8.x</i> <i>6.0.8.14.2 (P5)</i> <i>6.0.8.x (P1 – P15)</i> 6.0.8.25 (P16) 6.0.8.26 (P17)	<i>1.1.8.13</i> <i>1.1.8.16 – 24</i> <i>1.3.1.9 - 18</i> 1.3.1.21	<i>FND.C</i> FND.D - H
11.5.6	<i>8.1.6</i> <i>8.1.7.1</i> <i>8.1.7.2</i> <i>8.1.7.3</i> 8.1.7.4	<i>1.0.2.1.x*</i> 1.0.2.2.2	<i>6.0.8.8.x</i> <i>6.0.8.x (P1 – P15)</i> 6.0.8.25 (P16) 6.0.8.26 (P17)	<i>1.1.8.16 – 24</i> <i>1.3.1.9 - 18</i> 1.3.1.21	FND.D – H
11.5.7	<i>8.1.7.3</i> 8.1.7.4 <i>9.2.0.2</i> <i>9.2.0.3</i> <i>9.2.0.4</i> 9.2.0.5 9.2.0.6	<i>1.0.2.1.x*</i> 1.0.2.2.2	<i>6.0.8.18 (P9)</i> <i>6.0.8.x (P10 – P15)</i> 6.0.8.25 (P16) 6.0.8.26 (P17)	<i>1.1.8.16</i> <i>1.1.8.19 – 24</i> <i>1.3.1.9 - 18</i> 1.3.1.21	FND.E FND.F – H
11.5.8	8.1.7.4 <i>9.2.0.2</i> <i>9.2.0.3</i> <i>9.2.0.4</i> 9.2.0.5 9.2.0.6	<i>1.0.2.1.x*</i> 1.0.2.2.2	<i>6.0.8.18 (P9)</i> <i>6.0.8.x (P10 – P15)</i> 6.0.8.25 (P16) 6.0.8.26 (P17)	<i>1.1.8.16</i> <i>1.1.8.19 – 24</i> <i>1.3.1.9 - 18</i> 1.3.1.21	FND.F FND.G – H
11.5.9	<i>9.2.0.2</i> <i>9.2.0.3</i> <i>9.2.0.4</i> 9.2.0.5 9.2.0.6 10.1.0.4	<i>1.0.2.1.x*</i> 1.0.2.2.2	<i>6.0.8.21 (P12)</i> <i>6.0.8.x (P9 – P15)</i> 6.0.8.25 (P16) 6.0.8.26 (P17)	<i>1.1.8.16</i> <i>1.1.8.19 – 24</i> <i>1.3.1.9 - 18</i> 1.3.1.21	FND.G FND.H
11.5.10	<i>9.2.0.4</i> 9.2.0.5 9.2.0.6 10.1.0.4	<i>1.0.2.1.x*</i> 1.0.2.2.2	<i>6.0.8.24 (P15)</i> 6.0.8.25 (P16) 6.0.8.26 (P17)	<i>1.1.8.19 – 24</i> <i>1.3.1.18</i> 1.3.1.21	FND.H

\* Denotes version from fresh install

Note: All versions are based Sun Solaris and may differ slightly based on operating system and other factors. Please use the Certify tool in Oracle Metalink and the CPU installation notes for determining the exact supported versions for your platform.

## Oracle Database Patches

---

The database portion of the patch fixes over 29 security related bugs in many components of the database. The database portion of the patch is straight forward. The Oracle HTTP Server (OHS) may be installed if you have upgraded to Oracle 9iR2, thus, the mod\_plsql component patch may have to be installed.

Oracle Database security patches are cumulative, therefore, the patches for the previous CPUs (January 2005, April 2005, July 2005) and Oracle Security Alert #68 are included. Patches for all previous Oracle security alerts are also included in the database patch. See Metalink Note 237007.1 "FAQ for Security Alerts and Critical Patch Updates" question #13 for more details on the exact patches included in each update.

### *Testing*

An abbreviated testing cycle should be performed similar to testing for a minor database updated (e.g., 9.2.0.4 to 9.2.0.5). We can not provide specific recommendations as to where to focus testing efforts since the database patch touches all aspects of the database. For Microsoft Windows, the database patch is not a security specific patch and includes many non-security related fixes.

## Oracle Application Server Patches

---

### *1.0.2.1.x*

The patches for the Oracle Application Server require 1.0.2.1.x environments to upgrade to 1.0.2.2.x is significant as this upgrade requires a full installation of 1.0.2.2.x and implementation of AutoConfig as well as the installation of the latest Developer 6i PatchSet. All implementations installed using Rapid Install from 11.5.1 to 11.5.5 must upgrade or have previously upgraded in order to install the security patch.

### *1.0.2.2.x*

The CPU requires the 1.0.2.2.x Oracle Home be upgraded to 8.1.7.4, if already not done so. Patch 4572278 is cumulative for all previous CPUs.

### *Testing*

Since these patches impact both the Apache and JInitiator, a brief walk-through and execution of critical web pages and Forms should be performed to test the patches.

No additional testing should be required for the mod\_plsql component of the patch.

## Oracle Developer 6i Patches

---

There are no new vulnerabilities in Developer 6i, but Oracle requires Patchset 16 or 17 be applied to fix issues in previous CPUs and also as a prerequisite of the patch to the 8.0.6 Oracle Home.

## Oracle JInitiator Patches

---

There are no new vulnerabilities in Oracle JInitiator.

## Oracle E-Business Suite Patches

---

Most implementations will be required to apply around 10 E-Business Suite patches, with at least two of these patches being significant. Additional patches are required for sites running HR Self-Service.

The most significant patch is the Oracle Applications DBA (AD) Minipack I.1 or I.2. This patch requires the implementation of AutoConfig and updates the AutoConfig templates. Oracle has been slowing correcting security weaknesses in the standard Oracle Applications configuration by making minor changes to the AutoConfig templates, thus upgrading the to the latest and more secure templates.

The Workflow patches listed in Tables 5b and 5c of the Pre-installation Notes are an upgrade to the workflow processing to correct security issues.

The remainder of the patches either correct individual security vulnerabilities or cleanup inherent security weaknesses. Even if Oracle CRM Gateway for Mobile Devices, SDP Number Portability, Service, or Service Fulfillment Manager are not used or configured, the patches must be applied. The vulnerabilities corrected by these patches can be exploited even if the modules are not configured or used.

If you are running Oracle HR Self-Service, the patches listed in Table 5d of the Pre-installation Notes need to be applied. These patches correct security issues in the access of certain Self-Service web pages. We do not believe these issues are exploitable if HR Self-Service is not configured.

The CPU October 2005 patches are NOT cumulative for Oracle Applications, therefore, all the patches specified in the CPUs for January 2005, April 2005, and July 2005 also have to be applied if not already applied.

### ***Testing***

#### **AD Minipack (AD.I.1 or AD.I.2)**

Due to the nature of the Oracle Applications DBA (AD) Minipack, all functionality needs to be quickly tested after applying the Minipack. This testing should concentrate on access to functionality, rather than actual business flows (can you access the web page, run ADI, view reports, etc.). Testing should be especially rigorous if implementing AutoConfig, upgrading from an older AD version, or upgrading the AutoConfig templates from an older version.

#### **Workflow Patches (Table 5b and 5c)**

Testing of the Workflow patches should focus on verifying that workflow processes are functioning properly, notification mailer works, and any custom workflows are still in place. This testing should be similar in nature to testing a Workflow Minipack (i.e., OWF.G).

### Oracle HR Self Service Patches (Table 5d)

Functional testing should be performed on the “My Information” and “My Employee Information” – similar in nature to testing of a Minipack that may affect functionality.

### Other Patches

We do not have any specific testing recommendations for the other patches in the CPU as these patches affect only isolated technical components or fix specific security vulnerabilities in a limited set of files.

## Patching Strategy

With the number of patches required and testing effort, the patches need to be prioritized. A number of factors will affect the order and timing of the patches –

- Are the Oracle Applications servers directly connected to the Internet?
- Does the Oracle Applications database contain sensitive data (employee information, credit card numbers, etc.)?
- Is the internal network secure?
- Can anyone directly connect to the database and execute SQL statements?
- Is there a large technical or Oracle skilled user population?

Every organization and Oracle Applications environment is unique and will have individual requirements, testing procedures, and criteria for applying security patches. The following guidelines are meant to be a reference and guide to assist you in determining how you will apply the patches.

Many of the security vulnerabilities fixed in the CPU are risk high and need to be resolved quickly. All organizations should apply all the patches recommended by Oracle as soon as possible. However, based on operational realities and patching constraints of most Oracle Applications environments, some organizations may be willing to accept the risk of not immediately patching all these security vulnerabilities.

Our recommended patching strategy differs from Oracle's recommendation of applying the database server patches, then application server patches, and finally the Oracle Applications patches. We believe our strategy will provide faster resolution of the most critical security risks, although it will leave some high risk issues unpatched for a period of time.

### High Risk and Secure Environment Strategy

This strategy assumes all patches from previous CPUs and security alerts have already been applied. The following information is generalized for all versions of Oracle Applications 11i (11.5.1 to 11.5.10 CU2) and the exact patches will depend on your version of Oracle Applications.

**As soon as possible**

1. Apply the Oracle Database security patches as soon as possible. See Table 1 of the Pre-installation Notes for the exact patch for your version of the Oracle Database. We recommend all implementations prioritize this patch as critical.
2. Apply the following Oracle E-Business Suite patches as soon as possible –
  - o 3904641
  - o 4522020 or 4522035
  - o 4613714
  - o 4239060 or 4239066 or 4239070
3. Review the readme for patch 4537307 and if possible disable the Oracle Reports Server. We strongly encourage all implementations disable the Reports Server if feasible. Apply patch 4537307 as soon as possible.

**Next Scheduled Downtime**

4. Apply the following Oracle E-Business Suite patches during the next scheduled downtime where other patches will be applied –
  - o 4566995
  - o 4452532 or 4547026
  - o Workflow patches (Table 5b and 5c)
5. If running Oracle HR Self Service, apply the patches from Table 5d during the next scheduled downtime.

**Next Schedule Downtime or Upgrade Cycle**

6. Apply Oracle HTTP Server patch 4572278, which assumes the Application Server has been upgraded to 1.0.2.2.2 and its Oracle Home to 8.1.7.4. If Oracle Applications is directly connected to the Internet, you should prioritize this patch and apply it during the next scheduled downtime.
7. Apply the Oracle Applications DBA Minipack (AD.I.1 (4229931) or AD.I.2 (4337683)). This Minipack requires an upgrade to AutoConfig and upgrades the AutoConfig templates.
8. Apply Oracle Developer 6i Patchset 16 or 17, if already not done so. Apply the Developer 8.0.6 Oracle Home patches. See Table 3 for details.
9. Apply the JInitiator patches, if already not done so. See Table 4 for details.

**Non-High Risk Environment Strategy**

---

This strategy assumes some patches from previous CPUs and security have not been applied. The following information is generalized for all versions of Oracle Applications 11i (11.5.1 to 11.5.10 CU2) and the exact patches will be dependent on your version of Oracle Applications. There may be other dependencies and requirements (such as upgrading to FND.D) for your version of Oracle Applications. Due to the complexity and number of versions, it is not feasible to provide detailed guidance for every version in this analysis.

**Next Scheduled Downtime**

1. Apply the Oracle Database security patch. See Table 1 of the Pre-installation Notes for the exact patch for your version of the Oracle Database. We recommend all implementations prioritize this patch as critical. This patch is cumulative, therefore, all prior CPUs and security alerts are included. Applying this patch will provide the greatest benefit, especially if previous database security patches have not been applied.
2. Review the readme for patch 4537307 and if possible disable the Oracle Reports Server. We strongly encourage all implementations to disable the Reports Server if it is not being used. Apply patch 4537307.

**Next Scheduled Patch Cycle**

3. Apply the following Oracle E-Business Suite patches from this and previous CPUs, if not already applied. Oracle E-Business Suite security patches are not cumulative. See Metalink Note 315713.1 for more details on previous Oracle E-Business Suite security patches. All the patches from previous CPUs and security alerts are prioritized due to the length of time since release, even though some of these patches do not correct high risk vulnerabilities.

Previous Security Alerts (Metalink Note 315713.1)	<ul style="list-style-type: none"> <li>▪ 2326606</li> <li>▪ 2609399</li> <li>▪ 2782945</li> <li>▪ 2939083</li> <li>▪ 2919943</li> <li>▪ 3644626</li> </ul>
CPU January 2005	<ul style="list-style-type: none"> <li>▪ 1632947</li> <li>▪ 2343999</li> </ul>
CPU April 2005	<ul style="list-style-type: none"> <li>▪ 3748678</li> <li>▪ 4092100</li> <li>▪ 3803148</li> </ul>
CPU July 2005 (Requires FND.D)	<ul style="list-style-type: none"> <li>▪ 3966175</li> <li>▪ 4074867</li> <li>▪ 4388633</li> <li>▪ 4203332</li> <li>▪ 4094411</li> <li>▪ 4345226</li> </ul>
CPU October 2005	<ul style="list-style-type: none"> <li>▪ 3904641</li> <li>▪ 4522020 or 4522035</li> <li>▪ 4613714</li> <li>▪ 4239060 or 4239066 or 4239070</li> <li>▪ 4566995</li> <li>▪ 4452532 or 4547026</li> <li>▪ Workflow patches (Table 5b and 5c)</li> </ul>

4. If running Oracle HR Self Service, apply the patches from Table 5d during the next scheduled downtime.

## **Next Upgrade Cycle**

5. Apply Oracle HTTP Server patch 4572278, which assumes the Application Server has been upgraded to 1.0.2.2.2 and its Oracle Home to 8.1.7.4. If Oracle Applications is directly connected to the Internet, you should prioritize this patch and apply it during the next scheduled downtime.
6. Apply the Oracle Applications DBA Minipack (AD.I.1 (4229931) or AD.I.2 (4337683)). This Minipack requires an upgrade to AutoConfig and upgrades the AutoConfig templates.
7. Apply Oracle Developer 6i Patchset 16 or 17, if already not done so. Apply the Developer 8.0.6 Oracle Home patches. See Table 3 for details.
8. Apply the JInitiator patches, if already not done so. See Table 4 for details.

## About Integrigy Corporation

Integrigy Corporation is a leader in application security for large enterprise, mission critical applications. Our application vulnerability assessment tool, AppSentry, assists companies in securing their largest and most important applications. AppDefend is an intrusion prevention system for Oracle Applications and blocks common types of attacks against application servers. Integrigy Consulting offers security assessment services for leading ERP and CRM applications.

AppSentry and AppDefend have been updated to detect and/or block the vulnerabilities addressed in the Oracle Critical Patch Update – October 2005.

For more information, visit [www.integrigy.com](http://www.integrigy.com)

Integrigy Corporation  
P.O. Box 81545  
Chicago, Illinois 60602 USA  
888/542-4802  
[www.integrigy.com](http://www.integrigy.com)

Copyright © 2005 Integrigy Corporation.

If you have any questions, comments or suggestions regarding this document, please send them via e-mail to [alerts@integrigy.com](mailto:alerts@integrigy.com).

Integrigy, AppSentry, and AppDefend are trademarks of Integrigy Corporation. Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Integrigy's Vulnerability Disclosure Policy - Integrigy adheres to a strict disclosure policy for security vulnerabilities in order to protect our clients. We do not release detailed information regarding individual vulnerabilities and only provide information regarding vulnerabilities that is publicly available or readily discernable. We do not develop or distribute any type of exploit code. We provide verification or testing instructions for specific vulnerabilities only if the instructions do not disclose the exact vulnerability or if the information is publicly available.

The Information contained in this document includes information derived from various third parties. While the Information contained in this document has been presented with all due care, Integrigy Corporation does not warrant or represent that the Information is free from errors or omission. The Information is made available on the understanding that Integrigy Corporation and its employees and agents shall have no liability (including liability by reason of negligence) to the users for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on the information and whether caused by reason of any error, negligent act, omission or misrepresentation in the Information or otherwise.

Furthermore, while the Information is considered to be true and correct at the date of publication, changes in circumstances after the time of publication may impact on the accuracy of the Information. The Information may change without notice.