CYBERSECURITY SOLUTIONS

# ImageGuard
# Image Content Filtering

CYBER READY

mailguard

# **ImageGuard**
# Image Content Filtering

### Detect illicit and inappropriate inbound and outbound content sharing

Never has the creation and distribution of images been easier. The growth of image capturing devices, smart phones, photo sharing sites and online storage options mean that an illicit image can be created, uploaded and distributed globally in seconds.

Images stored on networks and passing through corporate email systems are the legal responsibility of that company. This constitutes huge risk in terms of legal liability, potential sexual harassment lawsuits and reputational damage if email images are not monitored and filtered. Implementing ImageGuard, combined with an Acceptable Use Policy (AEP) governing employee network access, can mitigate the severe implications of employee misuse.

### Illegal Images

#### Trained to stop pornographic imagery

ImageGuard does not specifically target or identify images of an illegal nature. It is trained to identify pornography involving sex acts and can therefore detect inappropriate material of this nature. Combined with the awareness of an image management system, this generally will result in employees refraining from sharing inappropriate material and exposing your business to unanticipated risk.

### Preserve and Manage Bandwidth

#### Dissuade sharing of inappropriate content

Image files are, by nature, larger than text based office documents and therefore consume more bandwidth and storage. By deploying image filtering technology and dissuading employees from sending or storing inappropriate material on your network, your company can free up valuable network bandwidth.

### Preserve Email Archives

#### Prevent permanent storage of illicit material

Many organizations archive and store email using a secure archiving solution (like SafeGuard) to achieve regulatory compliance. Unless filtered, any email containing illicit and inappropriate material will be archived leaving a permanent record in your system.

### Your Duty of Care to Employees

#### Demonstrated commitment to a safe workplace

Implementation of an image management system within a company's network demonstrates that a company is serious about its duty of care to employees. In conjunction with an AUP the company can show that it employs best practice and strives for a safe and enjoyable work environment for all.

### Protect Employees from Themselves

#### Avoid disciplinary action and reputational damage

Even your most high profile and highly salaried employees can transmit and receive illicit and inappropriate content. Dismissal or disciplinary action for misuse can result in the loss of a highly valuable company asset, and may even lead to wider publicity and reputational damage. With an AUP and image management companies can protect against these incidents.

### Manage Control of Content

#### Provide greater visibility of content

Many Network Administrators will admit that they don't know what potentially damaging content is flowing in and out, or residing on their network. ImageGuard is a powerful tool allowing companies to control and secure their environment.

# Contact MailGuard

**GENERAL ENQUIRIES**
**Phone** +61 3 9694 4444

**SALES**
1300 30 44 30
expert@mailguard.com.au

**TECHNICAL SUPPORT**
**Australia** 1300 30 65 10
**United States** 888 848 2822
**United Kingdom** 0 800 404 8993

**HEAD OFFICE**
**MailGuard Pty Ltd**
198 Normanby Rd
Southbank VIC Australia 3006
**Phone** +61 3 9694 4444
**Fax** +61 3 9011 6144
**Email** info@mailguard.com.au

**REGISTERED BILLING OFFICE**
**MailGuard Pty Ltd**
68-72 York St
South Melbourne VIC Australia 3205

CYBER
READY

mailguard