To: The Chair and Senior Officer of Registered Social Landlords

22 October 2019

Dear colleague,

I am writing to you to inform you of some matters that have come to our attention in the course of our work and also to update you on how the current uncertainty with regard to Brexit affects our regulatory requirements.

Tenant and Resident Safety
We are engaging with a number of landlords who have been unable to demonstrate that they are meeting tenant and resident safety requirements such as the management of asbestos and electrical safety.

The governing bodies of these landlords did not get or seek appropriate assurance that their organisation was meeting its legal duties on tenant and resident safety.

Social landlords must ensure they meet all duties on tenant and resident safety and that they obtain appropriate assurance about their compliance with all relevant safety requirements and that they take prompt action to address any non-compliance.

You should advise us of any issue which seriously affects the interests and safety of tenants, people who are homeless or other service users through the notifiable events process.

Cyber Security
We have been advised of a small number of recent incidents of fraud against Scottish RSLs through cyber-attacks. In at least one case the attacker has gained access to the personal data of tenants and service users of the RSL.

Regulatory Standard 4 requires each RSL to identify risks to its objectives and have effective strategies and systems for risk management and mitigation. Many RSLs have effective risk management arrangements, however given the recent deliberate targeting of the sector, it would be appropriate to review the adequacy of your cyber security arrangements.

The Annex to this letter contains information from the National Cyber Security Centre (NCSC) setting out the five critical controls that NCSC recommends (as a minimum) and details on how to access further advice on cyber security.

Scottish Housing Regulator,
Buchanan House,
58 Port Dundas Road,
Glasgow
G4 0HF

www.scottishhousingregulator.gov.uk

The UK Information Commissioner has noted publicly that achieving 'Cyber Essentials' accreditation can assist with meeting data protection duties. Links with more information on this accreditation are contained in the Annex to this letter.

Cyber-threat is one of a number of critical business risks which have the potential to challenge an organisation's resilience. Senior executives or stakeholders in RSLs are most likely to be the target of cyber- attack, because of their access to valuable assets (usually money and information) and also their influence within the organisation.

Ensuring that there is senior-level focus on managing these risks, and devoting appropriate time and resource to doing so will help to safeguard the interests of tenants and service users and maintain effective internal controls in this area.

If you uncover any activities that you believe to be fraudulent, you should continue to advise us through our notifiable events process.

I should be grateful if you would draw this advice to the attention of appropriate staff within your organisation.

Brexit
You may recall that we wrote to RSLs in February with advice on planning for Brexit. We remain of the view that the advice given then remains appropriate in the current context.

You will want to explore the resilience in your business plan to help your organisation cope with the risks that Brexit, especially a no-deal Brexit, will bring. It is equally important that landlords are aware of, and actively consider, the potential impacts on their tenants and customers of any decisions they make on steps to mitigate these risks.

This is of course a difficult balance to achieve. This is why a renewed focus by landlords on cost efficiency and value for money is ever more important.

In doing this, you may find it helpful to refer to the advisory guidance that we issued on Business Planning in December 2015.

This is clearly a fluid and fast moving situation and we welcome any information from landlords of particular risks and issues that they are encountering.

If you have any questions on any of these matters please contact the lead regulator for your organisation or contact us.

Yours Sincerely

Ian Brennan
Director of Regulation

Scottish Housing Regulator,
Buchanan House,
58 Port Dundas Road,
Glasgow
G4 0HF

www.scottishhousingregulator.gov.uk

Annex

NCSC Examples of Fraud five critical network controls

(i) Boundary firewalls and internet gateways – information, applications and computers within the organisation's internal networks should be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

(ii) Secure configuration – computers and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

(iii) Access control – user accounts, particularly those with special access privileges (e.g. administrative accounts) should be assigned only to authorised individuals, managed effectively and provide the minimum level of access to applications, computers and networks.

(iv) Malware protection – Computers that are exposed to the internet should be protected against malware infection through the use of malware protection software.

(v) Patch management – Software running on computers and network devices should be kept up-to-date and have the latest security patches installed.

There are a range of ways of achieving independent assurance that these critical controls are in place. One widely available certification scheme is Cyber Essentials, which offers a mechanism, endorsed by the National Cyber Security Centre, for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions. Its effectiveness has been independently assessed and verified by researchers at Lancaster University. Proportionate advice is available for small and medium sized organisations (less than 250 staff) and for large organisations (those with over 250 staff) with additional material specifically for board members. There are two types of certification under this scheme:

■ Cyber Essentials requires the organisation to complete a self-assessment questionnaire, with responses independently reviewed by an external certifying body.

■ Cyber Essentials Plus covers the same requirements as Cyber Essentials, but tests of the systems are carried out by an external certifying body using a range of tools and techniques.

Further information can be found at:

https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security