A publication brought to you by Ihry Insurance Agency, Inc.

Ihry News

August 2018

Contact Us:

Devils Lake
701.662.5027

Hillsboro
701.636.2540

Hope
800.726.7929

Mahnomen
218.935.5830

McVille
701.322.5553

Towner
701.537.5942

West Fargo
701.492.2228

www.ihryins.com

Fall Lawn Care Schedule For Our Cool-Season Grass

Article provided by Ihry Insurance.

Fall lawn care is an important element of your overall lawn care schedule. While it helps maintain your lawn's health through the fall months, it serves an even more important function: it prepares your lawn for winter survival and preemptively prepares for spring revival.

Winter can be long and tough on your lawn, so your fall lawn care is essential to ensuring your lawn perks up, and greens up, in the spring. It is a springboard to ensure you start out the following spring on a good foot.

Let's explore your fall lawn care schedule for cool-season grasses.

What are Cool-Season Grasses?

In the simplest terms, cool-season grasses are grass types that thrive in areas with cold winters and hot summers.

Grown in the upper two-thirds of the United States, cool-season grasses:

- Grow best in 65-70 degree temperatures.
- Should be mowed at 3-4 inches (this height changes in fall, but we will cover that later)
- Include Kentucky bluegrass, ryegrass, and fescue.
- Can withstand extreme temperature fluctuations

Fall Lawn Care Schedule

Early Fall

Fall is the best time to overseed because the ground is still warm, moisture is more plentiful, nights are cool, and the sun is not as hot during the day.

While a complete overseed is probably not necessary and requires sewing seed throughout the entire lawn, it's the perfect time to tackle those bare spots, thin patches, and dead areas.

Here's how to do it:

1. Loosen soil (at least ¼ inch deep) and remove any dead grass.
2. Sprinkle grass seed and lightly rake the seed into the loose soil.
3. Apply fertilizer (24-0-10 slow release).
4. Water generously for remainder of fall.

Early fall is also the first of two fertilizing rounds. Just as grass roots need water to last the winter, they also benefit from a shot of the plant sugars. These sugars protect roots from freezing and give the entire plant the energy to bounce back in the spring.

Use a spreader to apply a 24-0-10 (nitrogen, phosphorus, potassium) slow-release fertilizer to your lawn.

Mid Fall

Mid fall is aeration time. Aeration loosens the soil, allows your lawn to breathe, and allows nutrients, water, and fertilizer to permeate into the root zone.

However, before aerating, take the time to dethatch your lawn. Thatch is simply organic buildup on the surface of your lawn. If too thick, this thatch can begin to suffocate your lawn. By dethatching, you are not only removing this buildup, but you are giving yourself an idea of what conditions your grass and soil and have been living under.

If dethatching reveals a large amount of thatch, core aeration is likely needed and will need to be done professionally. If dethatching reveals a benign amount of thatch, you should be able to get away with poking holes (3 inches deep) into your lawn with a pitchfork (make rows 6-12 inches apart).

Late Fall

As late fall gives way to beautiful leaves, these leaves will succumb to gravity and create a cozy blanket over your lawn.

Your main job now is to keep leaves and debris off your lawn. If you live in an area with old, massive trees you will want to bag as many of the leaves as possible. If the amount of leaves isn't overwhelming, simply mulch them with your lawn mower. The fresh organics of the mulched leaves will add nutrients into your soil (while this may turn to thatch later, it is presently beneficial).

It's also your job to apply your final round of fertilizer. However, this is the time to apply a weed killer/fertilizer combo. Fall is the best time to preemptively deal with weeds, so find a fall 'weed and feed' fertilizer.

Fall Mowing Tip

Fall is the time to lower your mowing height. While summer requires cutting grass at 3 to 4 inches, fall is the time to **cut your grass at 2 inches.**

Your grass no longer has to defend itself against extreme summer heat, and you want to ensure your grass won't become matted down underneath leaves and snow. This matting can lead to mold and overall unhealthiness.

Do not mow lower than 2 inches. Mowing too short is one of the quickest ways to destroy your lawn.

Ihry Insights

Article provided by Curtis Kaufman, Agency Manager
Ihry Insurance

Farm Bill- Update

Conference Negotiations Begin

- Congress has completed the procedural steps necessary to begin conference negotiations on the two 2018 farm bills produced by the House and Senate. Additionally, the Congressional Budget Office has updated its score of each bill.

- While traditionally in recess during the month of August, reports are that conference negotiations will take place and some in Congressional leadership are pushing for an aggressive timeline to complete work and pass the final

bill before the September 30, 2018 expiration of the 2014 Farm Bill.

$12 Billion USDA Farm Aid Package

U.S. Farmer's Aid Package Like an "Insurance Claim," says Perdue

Agriculture Secretary Sonny Perdue reiterated Monday that any aid checks to producers this fall likely won't make farmers financially whole, and USDA won't attribute every drop in commodity prices solely to trade complications.

- Perdue reiterated to reporters Monday that the checks won't make farmers financially whole. "That's been consistent to what we have said all along," Perdue said. "I liken it really to any kind of insurance claim." The secretary compared it to a situation such as a car accident or home destroyed where a person never feels "whole" when the check comes.
- Perdue said USDA's chief economist has models that can differentiate the impact of trade disruption from normal seasonal price volatility for a given crop.
- "I think we're just trying to make the expectation that if a farmer sees a $2 drop in soybean prices, then they should not necessarily expect a $2-per-bushel mitigation payment. I think that's what we're trying to say."
- One of the reasons details about the disaster payments may not come until late August is USDA officials are waiting to see if some of these trade battles are resolved between now and then and prices rally, Perdue said.

Enjoy The Harvest!

IT Consultants: Should Small Business Owners Have a BYOD Policy?

Article provided by The Hartford.

As smartphones, laptops, and tablets become more engrained in our society their impact on small businesses has increased. In fact, most of your employees probably own a smartphone and prefer to use it over a company phone.

In response to this growing trend, a recent survey found that 59% of organizations have Bring Your Own Device (BYOD) policies in place with another 13% planning to implement a policy in the future. This means, that as an IT consultant or advisor you may want to advise small business owners on instituting a secure (BYOD) policy, to help protect their business. To get started, you can consider these four tips.

1. Encourage business owners to embrace BYOD for its benefits rather than trying to prohibit it.

"If you go to any convention where BYOD is being dealt with or spoken of, the initial response is to ban them," Sarah Lahav, CEO of Tel Aviv, an Israel-based help desk software maker says. "But realistically, you can't." For instance, 96 percent of employees check e-mail using mobile devices, according to the study by Sage, an Irvine, California-based business management software firm. And there is no practical way for employers to stop workers from using personal devices to email through web-based services such as Gmail.

However, BYOD policies do not have to be bad for business. "Business owners like BYOD because it reduces the cost of buying, securing, and supporting mobile devices while maintaining the ability to flexibly respond to customers," says Lahav.

With this in mind, you may want to consider the potential benefits of BYOD policies even closer. Some benefits include:

- **Increased worker satisfaction.** Employees like using devices they're used to, know how to work, and prefer.
- **Saving money.** Employees pay for their own devices and the maintenance that goes along with them.
- **Increased productivity.** Employees are used to their own devices and therefore will be more productive when using them.
- **Less IT involvement.** Having employees take care of their own device's maintenance, will require less involvement and work from the information technology's (IT) department. This can help to increase the IT department's productivity.
- **Increased employee engagement.** When employees use their own mobile devices, they are more likely to work outside the office. They are also more likely to engage with each other outside of the office, which increases productivity and employee relations.

2. Be realistic about security and support.

Realize that BYOD users won't be as effective as in-house or out-sourced experts when it comes to securing and maintaining their devices. "You can say 'bring your own support,'" Lahav says. "But that's not recommended. It still keeps the security hazard out there.

In addition to lax security, Lahav adds, you'll find that self-supported users aren't likely to be able to connect to company networks or otherwise use their devices as effectively for business purposes compared to those with more support.

However, when employers don't budget to protect company data from BYOD vulnerabilities or to advise employees how to use them, BYOD brings security and support problems that neither small firms nor individual employees are well-equipped to handle. Sensitive data may be exposed in an unsecured employee smartphone, or a customer won't be served because an employee can't figure out how to use his or her new tablet to pull up price quotes. "It's a complete headache," Lahav says. It's also a headache that many small business owners prefer to ignore.

Security threats you may face with a BYOD policy are:

- **Unsecured wireless networks.** When employees use their mobile devices outside of work in an unsecure wireless network, security breaches may occur.
- **Data leakage.** Mobile devices and tablets are vulnerable to security attacks, especially when used on unsecure networks. BYOD policies allow important company information to travel with employees, increasing vulnerability.
- **Malware.** This can be installed unknowingly onto a person's device threatening the security of your company's important information.

- **Stolen or lost devices.** To be prepared in the event of a stolen or lost device, you'll want to safeguard all information. One way of doing this is by using encryption tactics. Encryption involves turning data into code, to help keep it secure. Those with unauthorized access will not be able to access the code. This can ultimately decrease security threats and breaches in small businesses.

Educating employees on how to protect their devices will decrease the total number of threats to security your business encounters. Employees should secure their devices by:

- Using strong passwords.
- Ensuring they use protected and secure Wi-Fi connections.
- Encrypting their device.
- Installing antivirus software.
- Backing up their data regularly.
- Keeping your device updated.

3. Tap into natural social support.

Employees possess significant collective expertise as day-to-day users of their own devices, Lahav notes. Have employees who carry similar smartphones, tablets, or other devices talk to each other to help solve security and use problems. "Those people can help one another, although IT is not the core of their business," she says.

You can work with your IT Department or consultants to establish your policy. When crafting your policy be sure to:

- Specify what devices are permitted. For instance, you will want to decide if mobile devices, laptops or iPads are allowed as well as other devices.
- Lay down a security policy. Security policies can include requirements about what Wi-Fi networks you can connect to and where you can connect to them. It can also outline where data from BYOD devices is stored and what software is required.
- Outline that you own the personal information stored on the servers that employee's access with their devices. This can come up when a phone needs to be wiped and there are personal pictures and other data included on the phone.
- Ban certain apps. Apps that don't align with your policies should be banned and communicated to employees. Apps that are frequently banned in the office include Dropbox and Google+.
- Establish an employee exit strategy. This will outline the removal of access tokens, email access, data, and other proprietary applications and information when an employee leaves the company.

4. Require some security on BYODs.

JD Sherry, vice president of technology and solutions for Tokyo-based Trend Micro, suggests that personal smartphones that are used to tap company networks be required to carry security software that can detect and deter malware that could steal login information or other sensitive data. "That has to happen to make the small biz owner feel comfortable," Sherry says.

For Androids, security software apps that are successful at detecting malware include:

- Trend Micro Mobile Security and Antivirus
- Avast Mobile Security
- Avira Antivirus Security for Android

For iPhones, you can use:

- Avira Mobile Security
- Mobile Security and Anti-Theft Protection for iPhone
- Lookout Security & Identify Protection

Security tips for BYOD policies include:

- **Secure access controls with passwords.** This is a fundamental and basic step to securing any device. Make sure that your passwords are unique and difficult to crack.
- **Secure your wireless network.** Your employees should only use secured and trusted wireless networks. In addition, to this you can set up notifications for users when they enter a new network. This way they won't connect to any unsecure networks unknowingly.
- **Control access.** Your IT and security departments can enable access control features. These will control access and app permissions. This allows the app to access only what is needed to function and nothing extra.
- **Back up device data.** This helps protect you from security breaches and threats. This is also useful when an employee's phone is lost or stolen.
- **Run antivirus software.** Your apps should be protected with antivirus software. This software detects and removes malicious or harmful malware that can breach security.

At minimum, small businesses should understand that, if BYOD doesn't present security problems now, it will soon. "Reality is that cyber-criminals are fully migrating to mobile device platforms," says Sherry. That means that all the security and support problems that have plagued desktop business systems are or will soon be found on personal devices used to access business data. That means something has to be done. And fortunately, it can be, as long as small business owners are talked to about it in ways they can understand.